

Unifying Hyper and Epistemic Temporal Logics

Laura Bozzelli¹, Bastien Maubert², and Sophie Pinchinat³

¹ UPM, Madrid, Spain – laura.bozzelli@fi.upm.es

² IRISA, Université de Rennes 1, France – bastien.maubert@irisa.fr

³ IRISA, Université de Rennes 1, France – sophie.pinchinat@irisa.fr

Abstract

In the literature, two powerful temporal logic formalisms have been proposed for expressing information flow security requirements, that in general, go beyond regular properties. One is classic, based on the knowledge modalities of epistemic logic. The other one, the so called hyper logic, is more recent and subsumes many proposals from the literature; it is based on explicit and simultaneous quantification over multiple paths. In an attempt to better understand how these logics compare with each other, we consider the logic KCTL* (the extension of CTL* with knowledge modalities and synchronous perfect recall semantics) and HyperCTL*. We first establish that KCTL* and HyperCTL* are expressively incomparable. Second, we introduce and study a natural linear past extension of HyperCTL* to unify KCTL* and HyperCTL*; indeed, we show that KCTL* can be easily translated in linear time into the proposed logic. Moreover, we show that the model-checking problem for this novel logic is decidable, and we provide its exact computational complexity in terms of a new measure of path quantifiers' alternation. For this, we settle open complexity issues for unrestricted quantified propositional temporal logic.

1 Introduction

Temporal logics provide a fundamental framework for the description of the dynamic behavior of reactive systems. Additionally, they support the successful model-checking technology that allow complex finite-state systems to be verified automatically.

Classic *regular* temporal logics such as standard LTL [18] or the more expressive CTL* [10] lack mechanisms to relate distinct paths or executions of a system. Therefore, they cannot express information-flow security properties which specify how information may propagate from inputs to outputs, such as non-interference [12] or opacity [4].

In the literature, two powerful temporal logic formalisms have been proposed for expressing such security requirements that, in general, go beyond regular properties.

One is classical and is based on the extension of temporal logic with the knowledge modalities of epistemic logic [11], which allow to relate paths that are observationally equivalent for a given agent. We consider KCTL*, the extension of CTL* with knowledge modalities under the synchronous perfect recall semantics (where an agent remembers the whole sequence of its observations, and the observations are time-sensitive) [14, 21, 19, 8]. This logic and its linear-time fragment, KLTL, can be used to specify secrecy policies [1, 13, 3].

The second framework is more recent [6] and allows to express properties of sets of execution traces, known as *hyperproperties*, useful to formalize security policies, such as noninterference and observational determinism. The general hyper logical framework introduced in [6] is based on a second-order logic for which model-checking is undecidable. More recently, fragments of this logic have been introduced [5], namely the logics HyperCTL* and HyperLTL, which extend CTL* and LTL by allowing explicit and simultaneous quantification over multiple paths. HyperCTL* represents a simple and natural non-regular extension of CTL* which admits a decidable model-checking problem and in which important information-flow security policies can be expressed. HyperCTL* also generalizes a related temporal logic



© ;

licensed under Creative Commons License CC-BY

Leibniz International Proceedings in Informatics

LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

introduced in [9]. Other logics for hyperproperties have been introduced in [17], but as pointed in [5], no general approach to verifying such logics exists.

Contribution. Our first goal in this paper is to compare the expressive power of hyper temporal logics and epistemic temporal logics. We establish by formal non-trivial arguments that HyperCTL^* and KCTL^* are expressively incomparable. More precisely, we prove that HyperLTL (resp., KLTL) cannot be expressed in KCTL^* (resp., HyperCTL^*), even with respect to the restricted class of finite-state Kripke structures. The main intuitions are as follows. On the one hand, differently from HyperCTL^* , KCTL^* cannot express a linear-time requirement, simultaneously, on multiple paths. On the other hand, unlike KCTL^* , HyperCTL^* cannot express requirements which relate at some timestamp an unbounded number of paths.

As a second contribution, we introduce and investigate a natural linear past extension of HyperCTL^* , denoted by HyperCTL_{lp}^* , to unify HyperCTL^* and KCTL^* . This extension is strictly more expressive than HyperCTL^* ; indeed, we show that KCTL^* can be easily translated in linear time into HyperCTL_{lp}^* . Like HyperCTL^* and KCTL^* , the finite-state model-checking problem for the novel logic is non-elementarily decidable, and we provide the exact complexity of this problem in terms of a variant of the standard alternation depth of path quantifiers. For this, we settle complexity issues for satisfiability of unrestricted Quantified Propositional Temporal Logic (QPTL) [20]. The optimal upper bounds for full QPTL are obtained by a sophisticated generalization of the standard automata-theoretic approach for QPTL in prenex normal form [20], which exploits a subclass of parity two-way alternating word automata. Our results also solve complexity issues for HyperCTL^* left open in [5]. Due to lack of space some proofs are omitted and can be found in the Appendix.

► **Remark.** In [5], an extension of the semantics of HyperCTL^* is also considered. In this setting, the path quantification can simulate quantification over propositional variables, and within this generalized semantics, KLTL can be effectively expressed in HyperCTL^* [5].

2 Preliminaries

For all $i, j \in \mathbb{N}$, let $[i, j] := \{h \in \mathbb{N} \mid i \leq h \leq j\}$. Fix a *finite* set AP of atomic propositions. A *trace* is a finite or infinite word over 2^{AP} . For a word w over some alphabet, $|w|$ is the length of w ($|w| = \infty$ if w is infinite), and for each $0 \leq i < |w|$, $w(i)$ is the i^{th} symbol of w .

Structures and tree structures. A *Kripke structure* (over AP) is a tuple $K = \langle S, s_0, E, V \rangle$, where S is a set of states, $s_0 \in S$ is the initial state, $E \subseteq S \times S$ is a transition relation such that for each $s \in S$, $(s, t) \in E$ for some $t \in S$, and $V : S \rightarrow 2^{\text{AP}}$ is an *AP-valuation* assigning to each state s the set of propositions in AP which hold at s . The mapping V can be extended to words over S in the obvious way. A path $\pi = t_0, t_1, \dots$ of K is an infinite word over S such that for all $i \geq 0$, $(t_i, t_{i+1}) \in E$. For each $i \geq 0$, $\pi[0, i]$ denotes the prefix of π leading to the i^{th} state, and $\pi[i, \infty]$ the suffix of π from the i^{th} state. A finite path of K is a prefix of some path of K . An *initial path* of K is a path starting from the initial state. We say that $K = \langle S, s_0, E, V \rangle$ is a *tree structure* if S is a prefix-closed subset of \mathbb{N}^* , $s_0 = \varepsilon$ (the root of K), and $(\tau, \tau') \in E \Rightarrow \tau' = \tau \cdot i$ for some $i \in \mathbb{N}$. States of a tree structure are also called *nodes*. For a Kripke structure K , $\text{Unw}(K)$ is the tree unwinding of K from the initial state. A *tree structure* is *regular* if it is the unwinding of some finite Kripke structure.

2.1 Temporal Logics with knowledge modalities

We recall the *non-regular* extensions, denoted by KCTL^* and KLTL , of standard CTL^* and LTL obtained by adding the knowledge modalities of epistemic logic under the *synchronous*

perfect recall semantics [14, 21, 19, 8]. Differently from the asynchronous setting, the synchronous setting can be considered time sensitive in the sense that it can model an observer who knows that a transition has occurred even if the observation has not changed.

For a finite set **Agts** of agents, formulas φ of KCTL* over **Agts** and AP are defined as:

$$\varphi ::= \top \mid p \mid \neg\varphi \mid \varphi \vee \varphi \mid X\varphi \mid \varphi U \varphi \mid \exists\varphi \mid K_a\varphi$$

where $p \in \text{AP}$, $a \in \text{Agts}$, X and U are the “next” and “until” temporal modalities, \exists is the CTL* existential path quantifier, and K_a is the knowledge modality for agent a . We also use standard shorthands: $\forall\varphi := \neg\exists\neg\varphi$ (“universal path quantifier”), $F\varphi := \top U \varphi$ (“eventually”) and its dual $G\varphi := \neg F\neg\varphi$ (“always”). A formula φ is a *sentence* if each temporal/knowledge modality is in the scope of a path quantifier. The logic KLTL is the LTL-like fragment of KCTL* consisting of sentences of the form $\forall\varphi$, where φ does not contain path quantifiers.

The logic KCTL* is interpreted over *extended* Kripke structures (K, Obs) , i.e., Kripke structures K equipped with an *observation map* $\text{Obs} : \text{Agts} \rightarrow 2^{\text{AP}}$ associating to each agent $a \in \text{Agts}$, the set $\text{Obs}(a)$ of propositions which are observable by agent a . For an agent a and a finite trace $w \in (2^{\text{AP}})^*$, the a -observable part $\text{Obs}_a(w)$ of w is the finite trace of length $|w|$ such that for all $0 \leq i < |w|$, $\text{Obs}_a(w)(i) = w(i) \cap \text{Obs}(a)$. Two finite traces w and w' are (*synchronously*) *Obs_a-equivalent* if $\text{Obs}_a(w) = \text{Obs}_a(w')$ (note that $|w| = |w'|$). Intuitively, an agent a does not distinguish prefixes of paths whose traces are Obs_a -equivalent.

Given a KCTL* formula φ , an extended Kripke structure $\Lambda = (K, \text{Obs})$, an *initial* path π of K , and a position i along π , the satisfaction relation $\pi, i \models_{\Lambda} \varphi$ for KCTL* is inductively defined as follows (we omit the clauses for the Boolean connectives which are standard):

$$\begin{aligned} \pi, i \models_{\Lambda} p & \Leftrightarrow p \in V(\pi(i)) \\ \pi, i \models_{\Lambda} X\varphi & \Leftrightarrow \pi, i+1 \models_{\Lambda} \varphi \\ \pi, i \models_{\Lambda} \varphi_1 U \varphi_2 & \Leftrightarrow \text{for some } j \geq i : \pi, j \models_{\Lambda} \varphi_2 \text{ and } \pi, k \models_{\Lambda} \varphi_1 \text{ for all } k \in [i, j-1] \\ \pi, i \models_{\Lambda} \exists\varphi & \Leftrightarrow \text{for some initial path } \pi' \text{ of } K \text{ such that } \pi'[0, i] = \pi[0, i], \pi', i \models_{\Lambda} \varphi \\ \pi, i \models_{\Lambda} K_a\varphi & \Leftrightarrow \text{for all initial paths } \pi' \text{ of } K \text{ such that} \\ & V(\pi[0, i]) \text{ and } V(\pi'[0, i]) \text{ are } \text{Obs}_a\text{-equivalent, } \pi', i \models_{\Lambda} \varphi \end{aligned}$$

(K, Obs) *satisfies* φ , written $(K, \text{Obs}) \models \varphi$, if there is an initial path π of K such that $\pi, 0 \models_{(K, \text{Obs})} \varphi$. Note that if φ is a *sentence*, then the satisfaction relation $\pi, 0 \models_{(K, \text{Obs})} \varphi$ is independent of π . One can easily show that KCTL* is bisimulation invariant and satisfies the tree-model property. In particular, $(K, \text{Obs}) \models \varphi$ iff $(\text{Unw}(K), \text{Obs}) \models \varphi$.

► **Example 1.** Let us consider the KLTL sentence $\varphi_p := \forall XFK_a \neg p$.

For all observation maps Obs such that $\text{Obs}(a) = \emptyset$, $(K, \text{Obs}) \models \varphi_p$ means that there is some non-root level in the unwinding of K at which *no* node satisfies p . This requirement represents a well-known non-regular context-free branching temporal property (see e.g. [2]).

2.2 Hyper Logics

In this subsection, first, we recall the hyper logics HyperCTL* and HyperLTL [5] which are non-regular extensions of standard CTL* and LTL, respectively, with a restricted form of explicit first-order quantification over paths of a Kripke structure. Intuitively, path variables are used to express a linear-temporal requirement, simultaneously, on multiple paths. Then, we introduce a linear-time past extension of HyperCTL*, denoted by HyperCTL*_{lp}. In this novel logic, path quantification is ‘memoryful’, i.e., it ranges over paths that start at the root of the computation tree (the unwinding of the Kripke structure) and either visit the current

node τ (*regular* path quantification), or visit a node τ' at the same level as τ (*non-regular* path quantification).

The logic HyperCTL* [5]. For a finite set VAR of *path variables*, the syntax of HyperCTL* formulas φ over AP and VAR is defined as follows:

$$\varphi ::= \top \mid p[x] \mid \neg\varphi \mid \varphi \wedge \varphi \mid \mathbf{X}\varphi \mid \varphi \mathbf{U} \varphi \mid \exists x.\varphi$$

where $p \in \text{AP}$, $x \in \text{VAR}$, and $\exists x$ is the *hyper* existential path quantifier for variable x . Informally, formula $\exists x.\varphi$ requires that there is an initial path π such that φ holds with x mapped to π , and the atomic formula $p[x]$ assert that p holds at the current position of the path bound by x . The hyper universal path quantifier $\forall x$ is defined as: $\forall x.\varphi := \neg\exists x.\neg\varphi$. A HyperCTL* formula φ is a *sentence* if each temporal modality occurs in the scope of a path quantifier and for each atomic formula $p[x]$, x is bound by a path quantifier. The logic HyperLTL is the fragment of HyperCTL* consisting of formulas in prenex form, i.e., of the form $Q_1x_1 \dots Q_nx_n.\varphi$, where $Q_1, \dots, Q_n \in \{\exists, \forall\}$ and φ does not contain path quantifiers.

We give a semantics for HyperCTL* which is equivalent to that given in [5], but is more suitable for a linear-past memoryful generalization. HyperCTL* formulas φ are interpreted over Kripke structures $K = \langle S, s_0, E, V \rangle$ equipped with a *path assignment* $\Pi : \text{VAR} \rightarrow S^\omega$ associating to each variable $x \in \text{VAR}$ an *initial path* of K , a variable $y \in \text{VAR}$ ($\Pi(y)$ represents the current path), and a position $i \geq 0$ (denoting the current position along the paths in Π). The satisfaction relation $\Pi, y, i \models_K \varphi$ is defined as follows (we omit the clauses for the Boolean connectives which are standard):

$$\begin{aligned} \Pi, y, i \models_K p[x] &\Leftrightarrow p \in V(\Pi(x)(i)) \\ \Pi, y, i \models_K \mathbf{X}\varphi &\Leftrightarrow \Pi, y, i+1 \models_K \varphi \\ \Pi, y, i \models_K \varphi_1 \mathbf{U} \varphi_2 &\Leftrightarrow \text{for some } j \geq i : \Pi, y, j \models_K \varphi_2 \text{ and } \Pi, y, k \models_K \varphi_1 \text{ for all } k \in [i, j-1] \\ \Pi, y, i \models_K \exists x.\varphi &\Leftrightarrow \text{for some initial path } \pi \text{ of } K \text{ such that } \pi[0, i] = \Pi(y)[0, i], \\ &\quad \Pi[x \leftarrow \pi], x, i \models \varphi \end{aligned}$$

where $\Pi[x \leftarrow \pi](x) = \pi$ and $\Pi[x \leftarrow \pi](y) = \Pi(y)$ for all $y \neq x$. K *satisfies* φ , written $K \models \varphi$, if there is a path assignment Π of K and $y \in \text{VAR}$ such that $\Pi, y, 0 \models_K \varphi$. If φ is a *sentence*, then the satisfaction relation $\Pi, y, 0 \models_K \varphi$ is independent of y and Π . Note that CTL* corresponds to the set of sentences in the one-variable fragment of HyperCTL*.

► **Example 2.** The HyperLTL sentence $\varphi_p := \exists x.\exists y. p[x] \mathbf{U} ((p[x] \wedge \neg p[y]) \wedge \mathbf{XG}(p[x] \leftrightarrow p[y]))$ asserts that there are $\ell > 0$ and two distinct initial paths π and π' such that p always holds along the prefix $\pi[0, \ell]$, p does not hold at position ℓ of π' , and for all $j > \ell$, the valuations of p at position j along π and π' coincide. This requirement is clearly non-regular.

The novel logic HyperCTL*_{lp}. The syntax of HyperCTL*_{lp} formulas φ is as follows:

$$\varphi ::= \top \mid p[x] \mid \neg\varphi \mid \varphi \wedge \varphi \mid \mathbf{X}\varphi \mid \mathbf{X}^-\varphi \mid \varphi \mathbf{U} \varphi \mid \varphi \mathbf{U}^-\varphi \mid \exists x.\varphi \mid \exists^G x.\varphi$$

where \mathbf{X}^- and \mathbf{U}^- are the past counterparts of the temporal modalities \mathbf{X} and \mathbf{U} , respectively, and $\exists^G x$ is the *general* (hyper) existential quantifier for variable x . We also use some shorthands: $\forall^G x.\varphi := \neg\exists^G x.\neg\varphi$ (“general universal path quantifier”), $\mathbf{F}^-\varphi := \top \mathbf{U}^-\varphi$ (“past eventually”) and its dual $\mathbf{G}^-\varphi := \neg\mathbf{F}^-\neg\varphi$ (“past always”). The notion of sentence is defined as for HyperCTL*. The semantics of the modalities \mathbf{X}^- , \mathbf{U}^- , and $\exists^G x$ is as follows.

$$\begin{aligned} \Pi, y, i \models_K \mathbf{X}^-\varphi &\Leftrightarrow i > 0 \text{ and } \Pi, y, i-1 \models_K \varphi \\ \Pi, y, i \models_K \varphi_1 \mathbf{U}^-\varphi_2 &\Leftrightarrow \text{for some } j \leq i : \Pi, y, j \models_K \varphi_2 \text{ and } \Pi, y, k \models_K \varphi_1 \text{ for all } k \in [j+1, i] \\ \Pi, y, i \models_K \exists^G x.\varphi &\Leftrightarrow \text{for some initial path } \pi \text{ of } K, \Pi[x \leftarrow \pi], x, i \models \varphi \end{aligned}$$

The model-checking problem for HyperCTL_{lp}^* is checking given a *finite* Kripke structure K and a HyperCTL_{lp}^* sentence φ , whether $K \models \varphi$. It is plain to see that HyperCTL_{lp}^* is bisimulation invariant and satisfies the tree-model property. Hence, $K \models \varphi$ iff $\text{Unw}(K) \models \varphi$. Note that the set of sentences of the \exists^G -free one-variable fragment of HyperCTL_{lp}^* corresponds to the well-known equi-expressive linear-time memoryful extension CTL_{lp}^* of CTL^* [15].

We consider now two relevant examples from the literature which demonstrate the expressive power of HyperCTL_{lp}^* . Both examples rely on the ability to express observational equivalence in the logic: for an agent $a \in \text{Agts}$ and given two paths variables x and y in VAR , define $\text{Obs}_a(x, y) := G^-(\bigwedge_{p \in \text{Obs}(a)} p[x] \leftrightarrow p[y])$.

The first example shows that the logic can express *distributed knowledge*, a notion extensively investigated in [11]: a group of agents $A \subseteq \text{Agts}$ has distributed knowledge of φ , which we will write $D_A\varphi$, if the combined knowledge of the members of A implies φ . It is well known that the modality D_A cannot be expressed by means of modalities K_a [11]. Also, since HyperCTL^* cannot express the modality K_a (see Section 3.2), it cannot either express D_A . However, D_A is expressible in HyperCTL_{lp}^* : given a group of agents $A \subseteq \text{Agts}$ and a formula $\varphi \in \text{HyperCTL}_{lp}^*$, we define $\Pi, x, i \models_K D_A\varphi$ by $\Pi, x, i \models_K \forall^G y. [(\bigwedge_{a \in A} \text{Obs}_a(x, y)) \rightarrow \varphi]$.

The second example, inspired from [1], is an opacity requirement that we conjecture cannot be expressed neither in HyperCTL^* nor in KCTL^* . Assume that agent a can observe the low-security (boolean) variables p (i.e., $p \in \text{Obs}(a)$), but not the high-security variables p (i.e., $p \notin \text{Obs}(a)$). Consider the case of a secret represented by the value **true** of a high variable p_s . Then, the requirement $\forall x. G(p_s \rightarrow \forall^G y. \text{Obs}_a(x, y))$ says that whenever p_s holds at a node in the computation tree, all the nodes at the same level have the same valuations of low variables. Hence, the observer a cannot infer that the secret has been revealed.

3 Expressiveness issues

In this section, we establish that HyperCTL^* and KCTL^* are expressively incomparable. Moreover, we show that KCTL^* can be easily translated in linear time into HyperCTL_{lp}^* . As a consequence, HyperCTL_{lp}^* turns to be more expressive than both HyperCTL^* and KCTL^* .

Let \mathcal{L} be a logic interpreted over Kripke structures, \mathcal{L}' be a logic interpreted over *extended* Kripke structures, and C be a class of Kripke structures. For a sentence φ of \mathcal{L} , a sentence φ' of \mathcal{L}' , and an observation map Obs , φ and φ' are *equivalent w.r.t. C and Obs* , written $\varphi \equiv_{C, \text{Obs}} \varphi'$ if for all Kripke structures $K \in C$, $K \models \varphi$ iff $(K, \text{Obs}) \models \varphi'$. \mathcal{L}' is *at least as expressive as \mathcal{L} w.r.t. C* , written $\mathcal{L} \leq_C \mathcal{L}'$, if for every sentence φ of \mathcal{L} , there is an observation map Obs and a sentence φ' of \mathcal{L}' such that $\varphi \equiv_{C, \text{Obs}} \varphi'$. \mathcal{L} is *at least as expressive as \mathcal{L}' w.r.t. the class C* , written $\mathcal{L}' \leq_C \mathcal{L}$, if for every sentence φ' of \mathcal{L}' and for every observation map Obs , there is a sentence φ of \mathcal{L} such that $\varphi \equiv_{C, \text{Obs}} \varphi'$. Note the obvious asymmetry in the above two definitions due to the fact that for evaluating a sentence in \mathcal{L}' , we need to fix an observation map. If $\mathcal{L} \not\leq_C \mathcal{L}'$ and $\mathcal{L}' \not\leq_C \mathcal{L}$, then \mathcal{L} and \mathcal{L}' are *expressively incomparable w.r.t. C* . We write \leq_{fn} instead of \leq_C if C is the class of finite Kripke structures.

In order to prove that a given formula φ cannot be expressed in a logic \mathcal{L} , the naive technique is to build two models that φ can distinguish (i.e., φ evaluates to true on one model and to false on the other one), and prove that no formula of \mathcal{L} can distinguish those two models. A more involved technique, that we will use in the sequel in the expressiveness comparison between HyperCTL^* and KCTL^* , consists in building two families of models $(K_n)_{n \geq 1}$ and $(M_n)_{n \geq 1}$ such that φ distinguishes between K_n and M_n for all n , and for every formula ψ in \mathcal{L} , there is $n \geq 1$ such that ψ does not distinguish between K_n and M_n .

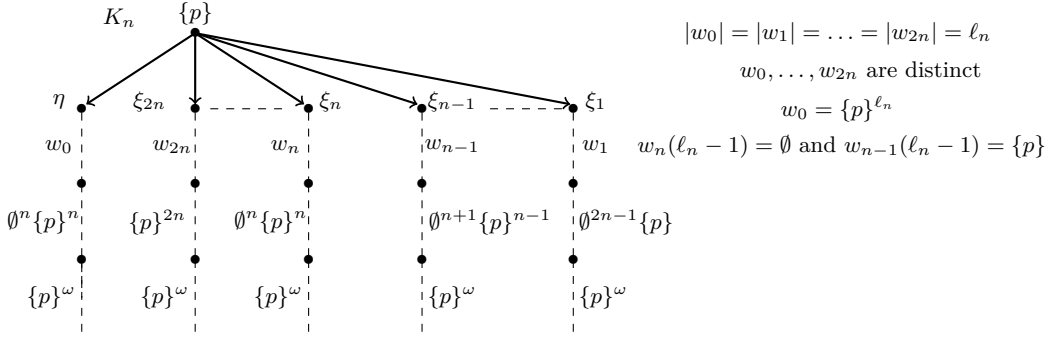
3.1 HyperCTL* is not subsumed by KCTL*

In this subsection, we show that HyperCTL* (and the LTL-like fragment HyperLTL as well) is not subsumed by KCTL* even if we restrict ourselves to the class of finite Kripke structures.

► **Theorem 3.** $\text{HyperLTL} \not\leq_{fin} \text{KCTL}^*$.

In order to prove Theorem 3, as witness HyperLTL sentence, we use the HyperLTL sentence φ_p of Example 2 given by $\varphi_p := \exists x. \exists y. p[x] \cup ((p[x] \wedge \neg p[y]) \wedge \text{XG}(p[x] \leftrightarrow p[y]))$.

We exhibit two families of *regular* tree structures $(K_n)_{n>1}$ and $(M_n)_{n>1}$ such that: (i) for all $n > 1$, φ_p distinguishes between K_n and M_n , and (ii) for every KCTL* sentence ψ , there is $n > 1$ such that ψ does *not* distinguish between (K_n, Obs) and (M_n, Obs) for all observation maps Obs . Hence, Theorem 3 follows. In the following, we fix $n > 1$.



■ **Figure 1** The regular tree structure K_n for the witness HyperLTL formula φ_p

► **Definition 4** (The regular tree structures K_n and M_n). K_n , which is illustrated in Fig. 1, is any regular tree structure over $2^{\{p\}}$ satisfying the following for some $\ell_n > 1$:

1. The root has label $\{p\}$ and $2n + 1$ successors $\eta, \xi_1, \dots, \xi_{2n}$, and there is a *unique* initial path visiting η (resp., ξ_k with $k \in [1, 2n]$). We denote such a path by $\pi(\eta)$ (resp., $\pi(\xi_k)$).
2. There are $2n + 1$ *distinct* finite words w_0, \dots, w_{2n} over $2^{\{p\}}$ of length ℓ_n such that:
 - $w_0 = \{p\}^{\ell_n}$, $w_n(\ell_n - 1) = \emptyset$ and $w_{n-1}(\ell_n - 1) = \{p\}$;
 - the trace of $\pi(\eta)$ is $\{p\} w_0 \emptyset^n \{p\}^n \{p\}^\omega$;
 - for all $k \in [1, 2n]$, the trace of $\pi(\xi_k)$ is $\{p\} w_k \emptyset^{2n-k} \{p\}^k \{p\}^\omega$.

M_n is obtained from K_n by replacing the label $\{p\}$ of the node $\pi(\xi_n)(\ell_n + 1 + n)$ with \emptyset . Note that in M_n , the traces of $\pi(\xi_n)[\ell_n + 1, \infty]$ and $\pi(\xi_{n-1})[\ell_n + 1, \infty]$ coincide.

In the regular tree structure K_n , the trace of the finite path $\pi(\eta)[0, \ell_n]$ is $\{p\}^{\ell_n+1}$, the label of $\pi(\xi_n)$ at position ℓ_n is \emptyset , and the traces of $\pi(\eta)[\ell_n + 1, \infty]$ and $\pi(\xi_n)[\ell_n + 1, \infty]$ coincide, which make $\pi(\eta)$ and $\pi(\xi_n)$ good candidates to fulfill φ_p . Hence:

► **Proposition 5.** $K_n \models \varphi_p$.

► **Proposition 6.** $M_n \not\models \varphi_p$.

Proof. The construction ensures that for all distinct initial paths π and π' and $\ell \in [0, \ell_n]$, the traces of $\pi[\ell, \infty]$ and $\pi'[\ell, \infty]$ in M_n are distinct (recall that $\pi(\xi_n)(\ell_n)$ and $\pi(\xi_{n-1})(\ell_n)$ have distinct labels). Moreover, $\pi(\eta)$ is the unique initial path of M_n such that for all $i \in [0, \ell_n]$, p holds at position i . Thus, since $\pi(\eta)(\ell_n + 1)$ has label \emptyset and there is no distinct initial path π'' of M_n such that the traces of $\pi(\eta)[\ell_n + 1, \infty]$ and $\pi''[\ell_n + 1, \infty]$ coincide, by construction of φ_p , the result easily follows. ◀

A KCTL* formula ψ is *balanced* if for every until subformula $\psi_1 \mathbf{U} \psi_2$ of ψ , it holds that $|\psi_1| = |\psi_2|$. By using the atomic formula \top , it is trivial to convert a KCTL* sentence ψ into an *equivalent* balanced KCTL* sentence of size at most $|\psi|^2$. This observation together with Propositions 5 and 6, and the following non-trivial result provide a proof of Theorem 3.

► **Theorem 7.** *Let ψ be a balanced KCTL* sentence such that $|\psi| < n$. Then, for all observation maps Obs , $(K_n, Obs) \models \psi \Leftrightarrow (M_n, Obs) \models \psi$.*

Proof. A full proof is in Appendix A.1. Let Obs be an observation map. Evidently, it suffices to show that for all initial paths π and positions $i \in [0, \ell_n]$, $\pi, i \models_{K_n, Obs} \psi$ iff $\pi, i \models_{M_n, Obs} \psi$. The key for obtaining this result is that since $|\psi| < n$, ψ cannot distinguish the nodes $\pi(\xi_n)(\ell_n + 1)$ and $\pi(\xi_{n-1})(\ell_n + 1)$ both in (K_n, Obs) and in (M_n, Obs) . For M_n , this indistinguishability easily follows from the construction and is independent of the size of ψ . For K_n , the indistinguishability is non-trivial and is formally proved by defining equivalence relations on the set of nodes at distance $d \in [\ell_n + 1, \ell_n + 2n]$ from the root, which are parameterized by a natural number $h \in [1, n]$, where h intuitively represents the size of the current balanced subformula of ψ in the recursive evaluation of ψ on K_n . ◀

3.2 KCTL* is not subsumed by HyperCTL*

In this Subsection, we show that KCTL* (and the LTL-like fragment KLTL as well) is not subsumed by HyperCTL* even with respect to the the class of finite Kripke structures.

For $p \in \text{AP}$, an observation map Obs is *p-blind* if for all agents a , $p \notin Obs(a)$.

► **Theorem 8.** *KLTL $\not\subseteq_{fin}$ HyperCTL*.*

As witness KLTL sentence for Theorem 8, we use the KLTL sentence φ_p of Example 1 given by $\varphi_p := \forall \text{XFK}_a \neg p$. We exhibit two families of *regular* tree structures $(K_n)_{n>1}$ and $(M_n)_{n>1}$ such that the following holds for all $n > 1$: (i) for each p -blind observation map Obs , φ_p distinguishes between (K_n, Obs) and (M_n, Obs) , and (ii) no HyperCTL* formula ψ of size less than n distinguishes between K_n and M_n . Hence, Theorem 8 follows.

Fix $n > 1$. In order to define K_n and M_n , we need additional definitions.

An *n-block* is a word in $\{p\}^*$ of length at least $n + 2$. Given finite words w_1, \dots, w_k over $2^{\{p\}}$ having the same length ℓ , the *join* $join(w_1, \dots, w_k)$ of w_1, \dots, w_k is the finite word over $2^{\{p\}}$ of length ℓ such that for all $i \in [0, \ell - 1]$, $join(w_1, \dots, w_k)(i) = w_1(i) \cup \dots \cup w_k(i)$. For a finite word w over $2^{\{p\}}$, the *dual* \tilde{w} of w is the finite word over $2^{\{p\}}$ of length $|w|$ such that for all $i \in [0, |w| - 1]$, $p \in \tilde{w}(i)$ iff $p \notin w(i)$.

Given n finite words w_1, \dots, w_n over $2^{\{p\}}$ of the same length, the tuple $\langle w_1, \dots, w_n \rangle$ *satisfies the n-fractal requirement* if for all $k \in [1, n]$, $join(w_1, \dots, w_k)$ has the form

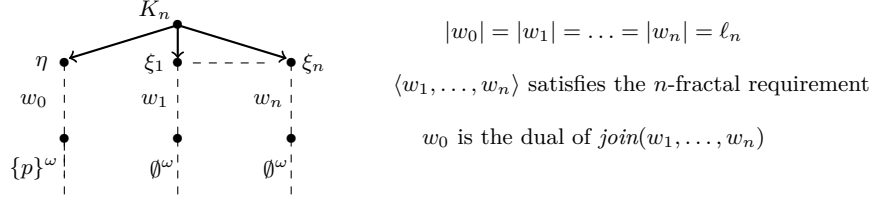
$$join(w_1, \dots, w_k) = bl_1^k \dots bl_{m_k}^k \cdot \{p\}$$

where $bl_1^k \dots bl_{m_k}^k$ are n -blocks. Moreover, $m_1 = n + 4$ and the following holds:

- if $k < n$, then w_{k+1} is obtained from $join(w_1, \dots, w_k)$ by replacing the last symbol with \emptyset , and by replacing each n -block bl_i^k of $join(w_1, \dots, w_k)$ by a sequence of $n + 4$ n -blocks preceded by a non-empty word in \emptyset^* of length at least $n + 2$.

► **Remark.** Assume that $\langle w_1, \dots, w_n \rangle$ satisfies the n -fractal requirement and let ℓ be the common length of w_1, \dots, w_n . Then, for all $i \in [0, \ell - 1]$, there is at most one $k \in [1, n]$ such that $p \in w_k(i)$. Moreover, $p \in w_1(0)$ and $p \in w_1(\ell - 1)$.

► **Definition 9** (The regular tree structures K_n and M_n). K_n , which is illustrated in Fig. 2, is any regular tree structure over $2^{\{p\}}$ satisfying the following for some $\ell_n > 1$:



■ **Figure 2** The regular tree structure K_n for the witness KTL formula $\varphi_p := \forall \text{XFK}_a \neg p$

1. The root has $n + 1$ distinct successors $\eta, \xi_1, \dots, \xi_n$ and there is a *unique* initial path visiting η (resp., ξ_k with $k \in [1, n]$). We denote such a path by $\pi(\eta)$ (resp., $\pi(\xi_k)$).
2. There are $n + 1$ finite words w_0, \dots, w_n of length ℓ_n such that:
 - the trace of $\pi(\eta)$ is $\emptyset w_0 \{p\}^\omega$ and for all $k \in [1, n]$, the trace of $\pi(\xi_k)$ is $\emptyset w_k \emptyset^\omega$;
 - $\langle w_1, \dots, w_n \rangle$ satisfies the n -fractal requirement and w_0 is the dual of $\text{join}(w_1, \dots, w_n)$.

A *main position* is a position in $[1, \ell_n]$. Let i_{alert} be the *third* (in increasing order) main position i along $\pi(\xi_1)$ such that the label of $\pi(\xi_1)(i)$ in K_n is $\{p\}$ (note that i_{alert} exists). Then, M_n is obtained from K_n by replacing the label $\{p\}$ of $\pi(\xi_1)$ at position i_{alert} with \emptyset .

By construction, in the regular tree structure K_n , for each non-root level, there is a node where p holds and a node where p does not hold. Hence:

► **Proposition 10.** *For each p -blind observation map Obs , $(K_n, \text{Obs}) \not\models \varphi_p$.*

By Remark 3.2, for each main position i , there is at most one $k \in [1, n]$ such that the label of $\pi(\xi_k)(i)$ in K_n is $\{p\}$. If such a k exists, we say that i is a *main p -position* and ξ_k is the *type* of i . Now, for the level of M_n at distance i_{alert} from the root, p *uniformly* does not hold (i.e., there is no node of M_n at distance i_{alert} from the root where p holds). Hence:

► **Proposition 11.** *For each p -blind observation map Obs , $(M_n, \text{Obs}) \models \varphi_p$.*

Theorem 8 directly follows from Propositions 10 and 11 and the following result.

► **Theorem 12.** *For all HyperCTL* sentences ψ such that $|\psi| < n$, $K_n \models \psi \Leftrightarrow M_n \models \psi$.*

Proof. A full proof is in Appendix A.2. The main idea is that for a HyperCTL* sentence ψ of size less than n , in the recursive evaluation of ψ on the tree structure M_n , there will be $h_* \in [2, n]$ such that the initial path $\pi(\xi_{h_*})$ is not bound by the current path assignment. Then, the n -fractal requirement ensures that in M_n , the main p -position i_{alert} (which in M_n has label \emptyset along $\pi(\xi_1)$) is indistinguishable from the main p -positions j of type ξ_{h_*} which are sufficiently ‘near’ to i_{alert} (such positions j have label \emptyset along the initial paths $\pi(\xi_k)$ with $k \neq h_*$). We formalize this intuition by defining equivalence relations on the set of main positions which are parameterized by h_* and a natural number $\mathbf{m} \in [0, n]$ and reflect the fractal structure of the main p -position displacement. Since the number of main p -positions of type ξ_1 following i_{alert} is at least n , we then deduce that in all the positions i such that $i \leq i_F$, where i_F is the main p -position of type ξ_1 preceding i_{alert} , no HyperCTL* formula ψ can distinguish M_n and K_n with respect to path assignments such that $|\Pi| + |\psi| < n$, where $|\Pi|$ is the number of initial paths bound by Π . Hence, the result follows. ◀

3.3 HyperCTL*_{lp} unifies KCTL* and HyperCTL*

We show that KCTL* can be easily translated in linear time into the two-variable fragment of HyperCTL*_{lp}. Intuitively, for a given observation map, the knowledge modalities can be

simulated by the general hyper path quantifiers combined with the temporal past modalities. Hence, we obtain the following result (for a detailed proof see Appendix A.3).

► **Theorem 13.** *Given a $KCTL^*$ sentence ψ and an observation map Obs , one can construct in linear time a $HyperCTL_{lp}^*$ sentence φ with just two path variables such that for each Kripke structure K , $K \models \varphi \Leftrightarrow (K, Obs) \models \psi$.*

By Theorems 3, 8, and 13, we obtain the following result.

► **Corollary 14.** *$HyperCTL_{lp}^*$ is strictly more expressive than both $HyperCTL^*$ and $KCTL^*$.*

4 Model-checking against $HyperCTL_{lp}^*$

In this section, we address the model-checking problem for $HyperCTL_{lp}^*$. Similarly to the proof given in [5] for the less expressive logic $HyperCTL^*$, we show that the above problem is non-elementarily decidable by linear time reductions from/to satisfiability of *full* Quantified Propositional Temporal Logic (QPTL, for short) [20], which extends LTL with past (PLTL) by quantification over propositions. As main contribution of this section, we address complexity issues for the considered problem by providing optimal complexity bounds in terms of a parameter of the given $HyperCTL_{lp}^*$ formula, we call *strong alternation depth*. For this, we first provide similar optimal complexity bounds for satisfiability of full QPTL. Our results also solve complexity issues for $HyperCTL^*$ left open in [5]. With regard to QPTL, well-known optimal complexity bounds in terms of the alternation depth of existential and universal quantifiers, concern the fragment of QPTL in prenex normal form (quantifiers cannot occur in the scope of temporal modalities) [20]. Unrestricted QPTL formulas can be translated in polynomial time into equivalent (with respect to satisfiability) QPTL formulas in prenex normal form, but in this conversion, the nesting depth of temporal modalities in the original formula (in particular, the alternation depth between always and eventually modalities and the nesting depth of until modalities) lead to an equal increasing in the quantifier alternation depth of the resulting formula. We show that this can be avoided by *directly* applying a non-trivial automatic theoretic approach to unrestricted QPTL formulas.

Syntax and semantics of QPTL. QPTL formulas φ over AP are defined as follows:

$$\varphi ::= \top \mid p \mid \neg\varphi \mid \varphi \wedge \varphi \mid X\varphi \mid X^-\varphi \mid \varphi U \varphi \mid \varphi U^-\varphi \mid \exists p.\varphi$$

where $p \in AP$. The positive normal form of a QPTL formula φ is obtained by pushing inward negations to propositional literals using De Morgan's laws and the duals R (release), R^- (past release), and $\forall p$ (propositional universal quantifier) of the modalities U, U^- , and $\exists p$. A formula is *existential* if its positive normal form does not contain universal quantifiers.

The semantics of QPTL is given w.r.t. (infinite) *pointed words* (w, i) over 2^{AP} consisting of an infinite word w over 2^{AP} and a position $i \geq 0$. All QPTL operators have the same semantics as in PLTL except for propositional quantification.

$$(w, i) \models \exists p.\varphi \Leftrightarrow \text{there is } w' \in (2^{AP})^\omega \text{ such that } w =_{AP \setminus \{p\}} w' \text{ and } (w', i) \models \varphi$$

where $w =_{AP \setminus \{p\}} w'$ means that the projections of w and w' over $AP \setminus \{p\}$ coincide. For a QPTL formula φ , we denote by $\mathcal{L}_p(\varphi)$ the set of pointed words (w, i) satisfying φ , and by $\mathcal{L}(\varphi)$ the set of infinite words w such that $(w, 0) \in \mathcal{L}_p(\varphi)$; φ is satisfiable if $\mathcal{L}(\varphi) \neq \emptyset$.

Optimal bounds for satisfiability of QPTL. First, we provide a generalization of the standard notion of alternation depth between existential and universal quantifiers in a QPTL

formula, we call *strong alternation depth*. This notion takes into account also the presence of temporal modalities occurrences between quantifier occurrences, but the nesting depth of temporal modalities is not considered (intuitively, it is collapsed to one).

► **Definition 15.** Let $\mathcal{O} = \{\exists, \forall, U, U^-, R, R^-, G, G^-, F, F^-\}$. First, we define the strong alternation length $\ell(\chi)$ of finite sequences $\chi \in \mathcal{O}^*$: $\ell(\varepsilon) = 0$, $\ell(Q) = 1$ for all $Q \in \mathcal{O}$, and

$$\ell(QQ'\chi) = \begin{cases} \ell(Q'\chi) & \text{if either } Q, Q' \in \mathcal{O} \setminus \{\exists, \forall\}, \text{ or } Q \in \{\exists, \forall\} \text{ and } Q' \in \mathcal{O} \setminus \{\exists, \forall\} \\ \ell(Q'\chi) & \text{if either } Q, Q' \in \{\exists, F, F^-\} \text{ or } Q, Q' \in \{\forall, G, G^-\} \\ 1 + \ell(Q'\chi) & \text{otherwise} \end{cases}$$

Then, the strong alternation depth $sad(\varphi)$ of a QPTL formula φ is the maximum over the strong alternation lengths $\ell(\chi)$, where χ is the sequence of modalities in \mathcal{O} along a path in the tree encoding of the positive normal form of φ .

Note that for a QPTL formula φ in prenex normal form, the strong alternation depth corresponds to the alternation depth of existential and universal quantifiers plus one. For all $n, h \in \mathbb{N}$, $\text{Tower}(h, n)$ denotes a tower of exponential of height h and argument n : $\text{Tower}(0, n) = n$ and $\text{Tower}(h + 1, n) = 2^{\text{Tower}(h, n)}$. We establish the following result, where $h\text{-EXPSPACE}$ is the class of languages decided by deterministic Turing machines bounded in space by functions of n in $O(\text{Tower}(h, n^c))$ for some constant $c \geq 1$.

► **Theorem 16.** *For all $h \geq 1$, satisfiability of QPTL formulas φ with strong alternation depth at most h is $h\text{-EXPSPACE}$ -complete, and $(h - 1)\text{-EXPSPACE}$ -complete in case φ is existential (even if the allowed temporal modalities are in $\{X, X^-, F, F^-, G, G^-\}$).*

Here, we illustrate the upper bounds of Theorem 16 (for the lower bounds see Appendix B.4). In the automata-theoretic approach for QPTL formulas φ in prenex normal form, first, one converts the quantifier-free part ψ of φ into an equivalent Büchi nondeterministic automaton (Büchi NWA) accepting $\mathcal{L}(\psi)$. Then, by using the closure under language projection and complementation for Büchi NWA, one obtains a Büchi NWA accepting $\mathcal{L}(\varphi)$. This approach does not work for unrestricted QPTL formulas φ , where quantifiers can occur in the scope of temporal modalities. In this case, for a subformula φ' of φ , we need to keep track of the full set $\mathcal{L}_p(\varphi')$ of pointed words (w, i) satisfying φ , and not simply $\mathcal{L}(\varphi')$.

Thus, we need to use *two-way* automata \mathcal{A} accepting languages $\mathcal{L}_p(\mathcal{A})$ of *pointed words*. In particular, the proposed approach is based on a compositional translation of QPTL formulas into the so called class of *simple two-way Büchi (nondeterministic) word automata* (Büchi SNWA). Essentially, given an input pointed word (w, i) , a Büchi SNWA, splits in two copies: the first one moves forwardly along the suffix $w[i, \infty]$ and the second one moves backwardly along the prefix $w[0, i]$ (see Appendix B.1 for details).

Moreover, at each step of the translation into Büchi SNWA, we use as an intermediate formalism, a two-way extension of the class of one-way hesitant *alternating* automata (HAA, for short) over infinite words introduced in [16]. Like one-way HAA, the set of states Q of a two-way HAA is partitioned into a set of components Q_1, \dots, Q_n such that moves from states in Q_i lead to states in components Q_j such that $j \leq i$. Moreover, each component is classified as either negative, or Büchi, or coBüchi: in a negative (resp., Büchi/coBüchi) component Q_i , the unique allowed moves from Q_i to Q_i itself are backward (resp., forward). These syntactical requirements ensure that in a run over a pointed word (w, i) , every infinite path π of the run gets trapped in some Büchi or coBüchi component, and the path π eventually use only forward moves. Moreover, the acceptance condition of a two-way HAA encodes a particular kind of parity condition of index 2: a Büchi/coBüchi component Q_i has associated

a subset $F_i \subseteq Q_i$ of accepting states. Then, a run is accepting if for every infinite path π , denoting with Q_i the Büchi/coBüchi component in which π get trapped, π satisfies the Büchi/coBüchi acceptance condition associated with Q_i . See Appendix B.1 for a formal definition of two-way HAA.

For two-way HAA, we establish two crucial results. First, for a two-way HAA \mathcal{A} , the dual automaton $\tilde{\mathcal{A}}$ obtained from \mathcal{A} by dualizing the transition function, and by converting a Büchi (resp., coBüchi) component into a coBüchi (resp., Büchi) component is still a two-way HAA. Thus, by standard arguments (see e.g. [22]), we obtain the following.

► **Lemma 17** (Complementation Lemma). *The dual automaton $\tilde{\mathcal{A}}$ of a two-way HAA \mathcal{A} is a two-way HAA accepting the complement of $\mathcal{L}_p(\mathcal{A})$.*

Second, by a non-trivial variation of the method used in [7] to convert parity two-way alternating word automata into equivalent Büchi NWA, we obtain the following result.

► **Theorem 18.** *For a two-way HAA \mathcal{A} with n states, one can construct “on the fly” and in singly exponential time a Büchi SNWA accepting $\mathcal{L}_p(\mathcal{A})$ with $2^{O(n \cdot \log(n))}$ states.*

The proof of Theorem 18 is in Appendix B.2. Finally, by using the complementation lemma for two-way HAA and Theorem 18, we establish the following Theorem 19 (whose proof is in Appendix B.3), from which the upper bounds of Theorem 16 directly follow (note that Büchi SNWA \mathcal{A} can be trivially converted into Büchi NWA accepting the set of infinite words w such that $(w, 0) \in \mathcal{L}_p(\mathcal{A})$, and for Büchi NWA checking nonemptiness is in NLOGSPACE). For a QPTL formula φ in positive normal form, if there is a universal quantified subformula $\forall p. \psi$ of φ such that $\text{sad}(\forall p. \psi) = \text{sad}(\varphi)$, we say that φ is a *first-level universal* formula; otherwise, we say that φ is a *first-level existential* formula.

► **Theorem 19.** *Let φ be a first-level existential (resp., first-level universal) QPTL formula and $h = \text{sad}(\varphi)$. Then, one can construct “on the fly” a Büchi SNWA \mathcal{A}_φ accepting $\mathcal{L}_p(\varphi)$ in time $\text{Tower}(h, O(|\varphi|))$ (resp., $\text{Tower}(h + 1, O(|\varphi|))$).*

Optimal bounds for model-checking of HyperCTL_{lp}^* . By giving linear-time reductions from/to satisfiability of QPTL and by exploiting Theorem 16, we provide optimal bounds on the complexity of the finite-state model-checking problem of HyperCTL_{lp}^* in terms of the *strong alternation depth* of a HyperCTL_{lp}^* formula, which is defined as the homonym notion for QPTL formulas. In particular, the linear time reduction to satisfiability of QPTL generalizes the one given in [5] for the model checking of HyperCTL^* (for details, see Appendix B.5).

► **Theorem 20.** *For all $h \geq 1$ and HyperCTL_{lp}^* sentences φ with strong alternation depth at most h , model-checking against φ is h -EXPSPACE-complete, and $(h-1)$ -EXPSPACE-complete in case φ is existential (even if the allowed temporal modalities are in $\{X, X^-, F, F^-, G, G^-\}$).*

5 Discussion

We plan to extend this work in many directions. We expand a few. First, we intend to identify tractable fragments of HyperCTL_{lp}^* and to investigate their synthesis problem; note that satisfiability of HyperCTL^* is already undecidable [5]. Second, we should extend the proposed framework in order to deal with asynchronicity, as this would allow us to considering more realistic information-flow security requirements. In the same line, we would like to investigate the possibility of extending the verification of flow-information requirements to relevant classes of infinite-state systems such as the class of pushdown systems, a model extensively investigated in software verification.

References

- 1 R. Alur, P. Černý, and S. Chaudhuri. Model checking on trees with path equivalences. In *Proc. 13th TACAS*, LNCS 4424, pages 664–678. Springer, 2007.
- 2 R. Alur, P. Černý, and S. Zdancewic. Preserving secrecy under refinement. In *Proc. 33rd ICALP*, LNCS 4052, pages 107–118. Springer, 2006.
- 3 M. Balliu, M. Dam, and G. Le Guernic. Epistemic temporal logic for information flow security. In *Proc. PLAS*, page 6. ACM, 2011.
- 4 J. Bryans, M. Koutny, L. Mazaré, and P.Y.A. Ryan. Opacity generalised to transition systems. *Int. J. Inf. Sec.*, 7(6):421–435, 2008.
- 5 M.R. Clarkson, B. Finkbeiner, M. Koleini, K.K. Micinski, M.N. Rabe, and C. Sánchez. Temporal logics for hyperproperties. In *Proc. 3rd POST*, LNCS 8414, pages 265–284. Springer, 2014.
- 6 M.R. Clarkson and F.B. Schneider. Hyperproperties. *Journal of Computer Security*, 18(6):1157–1210, 2010.
- 7 C. Dax and F. Klaedtke. Alternation elimination by complementation (extended abstract). In *Proc. 15th LPAR*, LNCS 5330, pages 214–229. Springer, 2008.
- 8 C. Dima. Revisiting satisfiability and model-checking for CTLK with synchrony and perfect recall. In *Proc. 9th CLIMA*, LNCS 5405, pages 117–131. Springer, 2008.
- 9 R. Dimitrova, B. Finkbeiner, M. Kovács, M.N. Rabe, and H. Seidl. Model checking information flow in reactive systems. In *Proc. 13th VMCAI*, LNCS 7148, pages 169–185. Springer, 2012.
- 10 E.A. Emerson and J.Y. Halpern. “Sometimes” and “not never” revisited: on branching versus linear time temporal logic. *Journal of the ACM*, 33(1):151–178, 1986.
- 11 R. Fagin, J.Y. Halpern, and M.Y. Vardi. *Reasoning about knowledge*, volume 4. MIT press Cambridge, 1995.
- 12 J.A. Goguen and J. Meseguer. Security policies and security models. In *IEEE Symposium on Security and privacy*, volume 12, 1982.
- 13 J.Y. Halpern and K.R. O’Neill. Secrecy in multiagent systems. *ACM Trans. Inf. Syst. Secur.*, 12(1), 2008.
- 14 J.Y. Halpern, R. van der Meyden, and M.Y. Vardi. Complete Axiomatizations for Reasoning about Knowledge and Time. *SIAM J. Comput.*, 33(3):674–703, 2004.
- 15 O. Kupferman, A. Pnueli, and M.Y. Vardi. Once and for all. *J. Comput. Syst. Sci.*, 78(3):981–996, 2012.
- 16 O. Kupferman, M.Y. Vardi, and P. Wolper. An Automata-Theoretic Approach to Branching-Time Model Checking. *Journal of ACM*, 47(2):312–360, 2000.
- 17 D. Milushev and D. Clarke. Towards incrementalization of holistic hyperproperties. In *Proc. 1st POST*, LNCS 7215, pages 329–348. Springer, 2012.
- 18 A. Pnueli. The temporal logic of programs. In *Proc. 18th FOCS*, pages 46–57. IEEE Computer Society, 1977.
- 19 N.V. Shilov and N.O. Garanina. Model checking knowledge and fixpoints. In *Proc. FICS*, BRICS Notes Series, pages 25–39, 2002.
- 20 A.P. Sistla, M.Y. Vardi, and P. Wolper. The complementation problem for Büchi automata with applications to temporal logic. *Theoretical Computer Science*, 49:217–237, 1987.
- 21 R. van der Meyden and N.V. Shilov. Model checking knowledge and time in systems with perfect recall (extended abstract). In *Proc. 19th FSTTCS*, LNCS 1738, pages 432–445. Springer, 1999.
- 22 W. Zielonka. Infinite games on finitely coloured graphs with applications to automata on infinite trees. *Theoretical Computer Science*, 200(1-2):135–183, 1998.

Appendix

A Proofs from Section 3

A.1 Proof of Theorem 7

In this Subsection, we prove the following result, where for the fixed $n > 1$, K_n and M_n are the regular tree structures over $2^{\{p\}}$ defined in Subsection 3.1.

► **Theorem 7.** *Let ψ be a balanced KCTL* sentence such that $|\psi| < n$. Then, for all observation maps Obs ,*

$$(K_n, Obs) \models \psi \Leftrightarrow (M_n, Obs) \models \psi$$

In order to prove Theorem 7, first, we give some definitions and preliminary results which capture some crucial properties of the regular tree structure K_n .

Recall that the sets of nodes of the regular tree structures K_n and M_n coincide. Thus, in the following, for node, we mean a node of K_n (or, equivalently, M_n). We denote by \preceq the partial order over the set of nodes defined as: $\tau \preceq \tau'$ iff there is path from τ visiting τ' . We write $\tau < \tau'$ to mean that $\tau \preceq \tau'$ and $\tau \neq \tau'$. For nodes τ and τ' , $Nodes(\tau, \tau')$ denotes the set of nodes τ'' such that $\tau \preceq \tau'' \preceq \tau'$. A *descendant* of a node τ is a node τ' such that $\tau' \succeq \tau$. By construction of K_n and M_n , for each non-root node τ , there is a unique initial path visiting τ . Such a path will be denoted by $\pi(\tau)$. In particular, τ has a unique successor which is denoted by $succ(\tau)$. For all observation maps Obs , KCTL* formulas ψ , and non-root nodes τ , we write $\tau \models_{K_n, Obs} \psi$ (resp., $\tau \models_{M_n, Obs} \psi$) to mean that $\pi(\tau), |\tau| \models_{K_n, Obs} \psi$ (resp., $\pi(\tau), |\tau| \models_{M_n, Obs} \psi$). Recall that $|\tau|$ is the distance of τ from the root.

Given an observation map Obs and an agent a , we say that two nodes τ and τ' are Obs_a -equivalent in K_n (resp., M_n) if the traces of the unique finite paths from the root to τ and τ' , respectively, are Obs_a -equivalent.

► **Definition 21 (Main nodes).** A *main position* is a position in $[\ell_n + 1, \ell_n + 2n]$.¹ A *main node* is a non-root node τ such that $\pi(\tau)$ visits τ at a main position (i.e., the distance $|\tau|$ of τ from the root is in $[\ell_n + 1, \ell_n + 2n]$).² A *main p-node* (resp., *main \emptyset -node*) is a main node whose label in K_n is $\{p\}$ (resp., \emptyset). For a \emptyset -main node τ , we denote by $p(\tau)$ the *smaller descendant* τ' of τ in K_n (with respect to the partial order \preceq) such that τ' is a p -main node. Note that by construction $p(\tau)$ is always defined. Moreover, for a main node τ , let $D(\tau)$ be the number of descendants of τ which are main nodes. The *order of a \emptyset -main node* τ is the number of descendants of τ in K_n which are \emptyset -main nodes.

Since the traces of $\pi(\eta)[1, \ell_n]$, $\pi(\xi_1)[1, \ell_n]$, \dots , $\pi(\xi_{2n})[1, \ell_n]$ are distinct, and the labels of K_n and M_n are in $2^{\{p\}}$, by construction, the following holds.

► **Remark.** For all observation maps Obs and agents a such that $p \in Obs(a)$, two main nodes τ and τ' are Obs_a -equivalent in K_n (resp., M_n) iff $\tau = \tau'$.

Now, for each $h \in [1, n]$, we introduce the crucial notion of h -compatibility between main nodes. Intuitively, this notion allows to capture the properties which make two main nodes indistinguishable from balanced KCTL* formulas of size at most h when evaluated on the regular tree structure K_n .

¹ Recall that ℓ_n is the common length of the words w_0, w_1, \dots, w_{2n} labeling $\pi(\eta)[1, \ell_n]$, $\pi(\xi_1)[1, \ell_n]$, \dots , $\pi(\xi_{2n})[1, \ell_n]$, respectively.

² See Fig. 1 for clarity.

► **Definition 22** (*h -Compatibility*). Let $h \in [1, n]$. Two main nodes τ and τ' are *h -compatible* if one of the following holds:

- τ and τ' are p -main nodes, and *either* $D(\tau) = D(\tau')$, *or* $D(\tau) \geq 2h$, $D(\tau') \geq 2h$, and $|D(\tau) - D(\tau')| = 1$;
- τ and τ' are \emptyset -main nodes, and one of the following holds, where $o(\tau)$ and $o(\tau')$ are the orders of τ and τ' :
 - $o(\tau) = o(\tau')$ and $D(\tau) = D(\tau')$;
 - $o(\tau) = o(\tau')$, $D(p(\tau)) \geq h$, $D(p(\tau')) \geq h$, $D(\tau) \geq 2h$, $D(\tau') \geq 2h$, $|D(\tau) - D(\tau')| = 1$;
 - $o(\tau) \geq h$, $o(\tau') \geq h$, $|o(\tau) - o(\tau')| = 1$, $D(\tau) \geq 2h$, $D(\tau') \geq 2h$, $|D(\tau) - D(\tau')| = 1$.

We denote by $R(h)$ the binary relation over the set of main nodes such that $(\tau, \tau') \in R(h)$ iff τ and τ' are h -compatible.

► **Remark.** For all $h \in [1, n]$, $R(h)$ is an equivalence relation.

The following two Propositions 23 and 24 capture some crucial properties of the equivalence relation $R(h)$. They are used in the next Lemma 25, two show that two h -compatible main nodes are indistinguishable from balanced KCTL* formulas of size at most h when evaluated on the regular tree structure K_n .

► **Proposition 23.** Let $h \in [2, n]$, $(\tau, \tau') \in R(h)$, and Obs be an observation map. Then, for all agents a and nodes τ_1 such that τ and τ_1 are Obs_a -equivalent in K_n , there exists a node τ'_1 such that τ' and τ'_1 are Obs_a -equivalent in K_n and $(\tau_1, \tau'_1) \in R(h-1)$.

Proof. Fix an observation map Obs . Let $h \in [2, n]$, $(\tau, \tau') \in R(h)$, and τ_1 be a node such that τ and τ_1 are Obs_a -equivalent in K_n . We prove that there exists a main node τ'_1 such that τ' and τ'_1 are Obs_a -equivalent in K_n and $(\tau_1, \tau'_1) \in R(h-1) \cup R(h)$. Thus, since $R(h) \subseteq R(h-1)$, the result follows. Note that τ_1 is a main node. If $p \in Obs(a)$, by Remark A.1, τ is the unique node which is Obs_a equivalent to τ itself. Hence, $\tau_1 = \tau$, and by setting $\tau'_1 = \tau'$, the result follows.

Now, assume that $p \notin Obs(a)$. Hence, two nodes are Obs_a -equivalent in K_n iff they have the same distance from the root. We assume that τ is a p -main node, hence, τ' is a p -main node as well. The case where τ is a \emptyset -main node is similar, and we omit the details here. In the rest of the proof, for a \emptyset -main node τ'' , we denote by $o(\tau'')$ the order of τ'' .

The case where $D(\tau) = D(\tau')$ is trivial (note that in this case, by construction, the main nodes τ and τ' have the same distance from the root). Now, assume that $D(\tau) \neq D(\tau')$. If τ_1 is a p -main node by setting $\tau'_1 = \tau'$, by construction, the result easily follows. Otherwise, τ_1 is a \emptyset -main node and $|\tau_1| = |\tau|$. Let τ_* be the node of $\pi(\tau_1)$ having the same distance from the root as τ' . If $(\tau_1, \tau_*) \in R(h-1)$, then by setting $\tau'_1 = \tau_*$, the result follows. Otherwise, since $(\tau, \tau') \in R(h)$, by construction, $D(\tau) \geq 2h$, $D(\tau') \geq 2h$, $|D(\tau) - D(\tau')| = 1$, and one of the following holds:

- $D(\tau) > D(\tau')$, $\tau_* = succ(\tau_1)$, and *either* $\tau_* = p(\tau_1)$, *or* τ_* is a \emptyset -main node, and $o(\tau_*) < h-1$: since $D(\tau_*) = D(\tau')$ (τ_* and τ' have the same distance from the root), we deduce that $D(p(\tau_1)) > 2h - (h-1) \geq h+1$. By construction, there exists a \emptyset -main node τ'_1 at the same distance from the root as τ_* such that $o(\tau'_1) = o(\tau_1)$ and $D(p(\tau'_1)) = D(p(\tau_1)) - 1$. Since $D(\tau_1) = D(\tau)$ and $D(\tau'_1) = D(\tau')$, we obtain that $(\tau_1, \tau'_1) \in R(h)$ and the result follows.
- $D(\tau) < D(\tau')$, $\tau_1 = succ(\tau_*)$, and $o(\tau_1) < h-1$: since $D(\tau_1) = D(\tau)$ (τ and τ_1 have the same distance from the root), we deduce that $D(p(\tau_1)) > 2h - (h-1) \geq h+1$. Since $o(\tau_*) \geq 2$, by construction, there exists a \emptyset -main node τ'_1 at the same level as τ_* such that $o(\tau'_1) = o(\tau_1)$, and $D(p(\tau'_1)) = D(p(\tau_1)) + 1$. Thus, since $D(\tau_1) = D(\tau)$ and $D(\tau'_1) = D(\tau')$, we obtain that $(\tau_1, \tau'_1) \in R(h)$ and the result follows.



For a real number r , $\lfloor r \rfloor$ denotes the integral part of r .

► **Proposition 24.** *Let $h \in [2, n]$, $(\tau, \tau') \in R(h)$, and τ_2 be a main node such that $\tau_2 \succeq \tau$. Then, the following holds:*

1. *either $\text{succ}(\tau)$ and $\text{succ}(\tau')$ are not main nodes, or $(\text{succ}(\tau), \text{succ}(\tau')) \in R(h-1)$;*
2. *there exists a main node $\tau'_2 \succeq \tau'$ such that $(\tau_2, \tau'_2) \in R(\lfloor \frac{h}{2} \rfloor)$ and the restriction of $R(\lfloor \frac{h}{2} \rfloor)$ to $\text{Nodes}(\tau, \tau_2) \times \text{Nodes}(\tau', \tau'_2)$ is total.³*

Proof. We use the following preliminary result.

Claim 1: Let $h \in [1, n]$, $(\tau, \tau') \in R(h)$ such that τ is a p -main node, and τ_2 be a main node such that $\tau_2 \succeq \tau$. Then, there exist a main node $\tau'_2 \succeq \tau'$ such that $(\tau_2, \tau'_2) \in R(h)$ and the restriction of $R(h)$ to $\text{Nodes}(\tau, \tau_2) \times \text{Nodes}(\tau', \tau'_2)$ is total.

Proof of Claim 1: Assume that $D(\tau) \neq D(\tau')$ (the other case being trivial). Since $(\tau, \tau') \in R(h)$, τ' is a p -main node as well. Moreover, $|D(\tau) - D(\tau')| = 1$, and $D(\tau) \geq 2h$ and $D(\tau') \geq 2h$. We focus on the case $D(\tau') = D(\tau) + 1$ (the other case when $D(\tau) = D(\tau') + 1$ being similar). By construction every main node which is a descendent of either τ or τ' is a p -main node. If $\tau_2 = \tau$, then by setting $\tau'_2 = \tau'$, the result trivially follows. Otherwise, let $\tau'_1 = \text{succ}(\tau')$. Note that τ'_1 is a p -main node and $D(\tau) = D(\tau'_1)$. Hence, the restriction of $R(h)$ to $\{\tau\} \times \{\tau', \tau'_1\}$ is total. Thus, by definition of $R(h)$, the result easily follows. ◀

Now, we prove Proposition 24.

Let $h \in [2, n]$, $(\tau, \tau') \in R(h)$, and τ_2 be a main node such that $\tau_2 \succeq \tau$. We prove Properties 1 and 2 by induction on $D(\tau)$.

For the base case, $D(\tau) = 1$. By definition of $R(h)$, we deduce that $D(\tau') = 1$ as well, hence, Properties 1 and 2 easily follow.

For the induction step, assume that $D(\tau) > 1$. Hence, $D(\tau') > 1$ as well. Since $(\tau, \tau') \in R(h)$, only the following two cases can occur:

- τ and τ' are p -main nodes: Property 2 directly follows from Claim 1 and the fact that $R(h) \subseteq R(\lfloor \frac{h}{2} \rfloor)$. Moreover, since $D(\tau) > 1$, $D(\tau') > 1$, and $(\tau, \tau') \in R(h)$, by definition of $R(h)$, Property 1 easily follows.
- τ and τ' are \emptyset -main nodes: Property 1 easily follows. Now, let us consider Property 2. Let $o(\tau)$ and $o(\tau')$ be the orders of τ and τ' . We distinguish two cases:
 - $o(\tau) \neq o(\tau')$: since $(\tau, \tau') \in R(h)$, $|o(\tau) - o(\tau')| = 1$, $o(\tau) \geq h$, $o(\tau') \geq h$, $D(\tau) \geq 2h$, $D(\tau') \geq 2h$, and $p(\tau)$ and $p(\tau')$ have the same distance from the root. Assume that $o(\tau) = o(\tau') + 1$ (the other case being similar). If $\tau_2 = \tau$, then by setting $\tau'_2 = \tau'$, the result trivially follows. Otherwise, let $\tau_1 = \text{succ}(\tau)$. Note that τ_1 is a \emptyset -main node and $D(\tau_1) = D(\tau')$. Hence, the restriction of $R(h)$ to $\{\tau, \tau_1\} \times \{\tau'\}$ is total. Thus, by definition of $R(h)$ and the fact that $R(h) \subseteq R(\lfloor \frac{h}{2} \rfloor)$, the result easily follows.
 - $o(\tau) = o(\tau')$: if $D(\tau) = D(\tau')$, the result easily follows. Otherwise, since $(\tau, \tau') \in R(h)$, $|D(p(\tau)) - D(p(\tau'))| = 1$, $D(p(\tau)) \geq h$ and $D(p(\tau')) \geq h$. Hence, $(p(\tau), p(\tau')) \in R(\lfloor \frac{h}{2} \rfloor)$. By construction, it easily follows that for each main node $\tau_1 \in \text{Nodes}(\tau, p(\tau))$, there exists $\tau'_1 \in \text{Nodes}(\tau', p(\tau'))$ such that $(\tau_1, \tau'_1) \in R(\lfloor \frac{h}{2} \rfloor)$ and the restriction of $R(\lfloor \frac{h}{2} \rfloor)$ to $\text{Nodes}(\tau, \tau_1) \times \text{Nodes}(\tau', \tau'_1)$ is total. Thus, since $p(\tau)$ and $p(\tau')$ are p -main nodes, by Claim 1, Property 2 follows.

³ Recall that a binary relation $R \subseteq S \times S'$ is total if for all $s \in S$ (resp., $s' \in S'$), there exists $s' \in S'$ (resp., $s \in S$) such that $(s, s') \in R$.

This concludes the proof of Proposition 24. \blacktriangleleft

► **Lemma 25.** *Let ψ be a balanced $KCTL^*$ formula such that $|\psi| \leq n$, Obs be an observation map, and $(\tau, \tau') \in R(|\psi|)$. Then,*

$$\tau \models_{K_n, Obs} \psi \Leftrightarrow \tau' \models_{K_n, Obs} \psi$$

Proof. Fix an observation map Obs . We use the following fact that directly follows from the semantics of $KCTL^*$ and the fact that in K_n , for every node τ such that τ is not a main node, and τ is a descendant of some main node, the trace of the unique path from τ is $\{p\}^\omega$.

Claim 1. Let τ and τ' be descendants of main nodes such that τ and τ' are not main nodes. Then, for each $KCTL^*$ formula,

$$\tau \models_{K_n, Obs} \psi \Leftrightarrow \tau' \models_{K_n, Obs} \psi$$

Now, we prove Lemma 25. Let ψ be a balanced $KCTL^*$ formula such that $|\psi| \leq n$ and $(\tau, \tau') \in R(|\psi|)$. We need to show that

$$\tau \models_{K_n, Obs} \psi \Leftrightarrow \tau' \models_{K_n, Obs} \psi$$

The proof is by induction on $|\psi|$. The cases for the boolean connectives \neg and \wedge , and the existential path quantifier \exists , directly follow from the inductive hypothesis and the fact that $R(h) \subseteq R(k)$ for all $h, k \in [1, n]$ such that $h \geq k$. For the other cases, we proceed as follows.

- Case $\psi = p'$ for some $p' \in AP$: since $(\tau, \tau') \in R(|\psi|)$, τ and τ' have the same label in K_n . Hence, the result follows.
- Case $\psi = X\psi'$. If $succ(\tau)$ and $succ(\tau')$ are not main nodes, the result directly follows from Claim 1. Otherwise, by applying Proposition 24(1), we obtain that $(succ(\tau), succ(\tau')) \in R(|\psi'|)$. Hence, in this case, the result directly follows from the induction hypothesis.
- $\psi = \psi_1 U \psi_2$: we focus on the implication $\tau \models_{K_n, Obs} \psi \Rightarrow \tau' \models_{K_n, Obs} \psi$ (the converse implication being symmetric). Let $\tau \models_{K_n} \psi$. Hence, there exists $\tau_2 \succeq \tau$ such that $\tau_2 \models_{K_n, Obs} \psi_2$ and $\tau_1 \models_{K_n, Obs} \psi_1$ for all nodes τ_1 such that $\tau \preceq \tau_1 \prec \tau_2$. We need to prove that $\tau' \models_{K_n, Obs} \psi$. We distinguish two cases:
 - τ_2 is a main node: since $(\tau, \tau') \in R(|\psi|)$, by applying Proposition 24(2), there exists a main node $\tau'_2 \succeq \tau'$ such that the restriction of $R(\lfloor \frac{|\psi|}{2} \rfloor)$ to $Nodes(\tau, \tau_2) \times Nodes(\tau', \tau'_2)$ is total and $(\tau_2, \tau'_2) \in R(\lfloor \frac{|\psi|}{2} \rfloor)$. Since ψ is balanced, $|\psi_1| = |\psi_2|$. Hence, for all $h = 1, 2$, $|\psi_h| \leq \lfloor \frac{|\psi|}{2} \rfloor$, and in particular, $R(|\psi_h|) \supseteq R(\lfloor \frac{|\psi|}{2} \rfloor)$. Hence, by applying the induction hypothesis, the result easily follows.
 - τ_2 is not a main node: let τ_* be the greatest (with respect to \preceq) ancestor of τ_2 which is a main node. Note that $\tau_* \succeq \tau$. By reasoning as in the previous case, there exists $\tau'_* \succeq \tau'$ such that for all $\tau_1 \in Nodes(\tau', \tau'_*)$, $\tau_1 \models_{K_n, Obs} \psi_1$ and $(\tau_*, \tau'_*) \in R(\lfloor \frac{|\psi|}{2} \rfloor)$. We show that $succ(\tau'_*) \models_{K_n, Obs} \psi$, hence, the result follows. Since $succ(\tau_*)$ is not a main node, by Proposition 24(1), $succ(\tau'_*)$ is not a main node as well. Thus, since $\tau_2 \models_{K_n, Obs} \psi$, by applying Claim 1, the result follows.
- $\psi = K_a \psi_1$. We focus on the implication $\tau \models_{K_n, Obs} \psi \Rightarrow \tau' \models_{K_n, Obs} \psi$ (the converse implication being symmetric). Assume that $\tau \models_{K_n, Obs} \psi$. Let τ'_1 be a node such that τ'_1 and τ' are Obs_a -equivalent in K_n . We need to show that $\tau'_1 \models_{K_n, Obs} \psi_1$. Since $(\tau, \tau') \in R(|\psi|)$ and $R(|\psi|)$ is an equivalence relation, by applying Proposition 23, there exists a main node τ_1 such that τ and τ_1 are Obs_a -equivalent in K_n , and $(\tau_1, \tau'_1) \in R(|\psi_1|)$. Since $\tau \models_{K_n, Obs} \psi$, it holds that $\tau_1 \models_{K_n, Obs} \psi_1$. Thus, by applying the induction hypothesis, the result follows.



Now, we can prove the crucial lemma from which Theorem 7 directly follows.

► **Lemma 26.** *Let ψ be a balanced $KCTL^*$ formula such that $|\psi| < n$ and Obs be an observation map. Then, for all initial paths π of K_n (or, equivalently, M_n) the following holds:*

1. $\pi, 0 \models_{K_n, Obs} \psi \Leftrightarrow \pi, 0 \models_{M_n, Obs} \psi$.
2. $\pi, i \models_{K_n, Obs} \psi \Leftrightarrow \pi, i \models_{M_n, Obs} \psi$ for all $i \in [1, \ell_n]$.
3. if π does not visit node ξ_n (i.e., $\pi \neq \pi(\xi_n)$), then for all $i \geq \ell_n + 1$,

$$\pi, i \models_{K_n, Obs} \psi \Leftrightarrow \pi, i \models_{M_n, Obs} \psi$$

Proof. First, we make the following observation which directly follows from the semantics of $KCTL^*$, Remark A.1, and the fact that for each observation map Obs and agent a such that $p \notin Obs(a)$, two nodes τ and τ' are Obs_a -equivalent in K_n (resp., M_n) iff $|\tau| = |\tau'|$ (i.e., τ and τ' have the same distance from the root).

Claim 1. Let $K \in \{K_n, M_n\}$, τ and τ' be two non-root nodes such that $|\tau| = |\tau'| \geq \ell_n + 1$ and in K , the traces of the unique paths starting from τ and τ' , respectively, coincide. Then, for all $KCTL^*$ formulas ψ and observation maps Obs :

$$\tau \models_{K, Obs} \psi \Leftrightarrow \tau' \models_{K, Obs} \psi$$

Now, we prove Properties 1–3 of Lemma 26. Fix an observation map Obs . Let ψ be a balanced $KCTL^*$ formula such that $|\psi| < n$ and π be an initial path of K_n (or, equivalently, M_n). The proof of Properties 1–3 is by induction on $|\psi|$. The case for atomic propositions directly follows from construction. The cases for negation, conjunction, and existential path quantifier directly follows from the induction hypothesis (recall that for each non-root node τ there is exactly one initial path visiting τ). For the remaining case, we proceed as follows.

- Cases $\psi = X\psi'$ or $\psi = \psi_1 U \psi_2$: assume that $\psi = \psi_1 U \psi_2$ (the case where $\psi = X\psi'$ being similar). For Property 1, we apply the induction hypothesis for Property 1, and Property 2 for the considered case. For Property 3, we apply the induction hypothesis on Property 3. Now, let us consider Property 2. The case where π does not visit ξ_n directly follows from the induction hypothesis on Properties 2 and 3. Now, assume that π visits node ξ_n , i.e. $\pi = \pi(\xi_n)$. Let τ_n be the first main node visited by $\pi(\xi_n)$. Note that τ_n is a \emptyset -main node and $\tau_n = \pi(\xi_n)(\ell_n + 1)$. Since $\tau_n \succ \xi_n$, by the semantics of the until modality and applying the induction hypothesis on Property 2, it suffices to show that

$$\tau_n \models_{K_n, Obs} \psi \Leftrightarrow \tau_n \models_{M_n, Obs} \psi$$

Let τ_{n-1} be the first main node visited by $\pi(\xi_{n-1})$, and $\tau'_{n-1} = succ(\tau_{n-1})$. Note that τ_{n-1} is a \emptyset -main node and $\tau_{n-1} = \pi(\xi_{n-1})(\ell_n + 1)$. By construction, we have that $(\tau_n, \tau'_{n-1}) \in R(n-1)$ and $(\tau_{n-1}, \tau'_{n-1}) \in R(n-1)$. Since $R(n-1) \subseteq R(|\psi|)$ (recall that $|\psi| < n$), by applying twice Lemma 25, we obtain

$$\tau_n \models_{K_n, Obs} \psi \Leftrightarrow \tau_{n-1} \models_{K_n, Obs} \psi$$

Moreover, since in M_n , the traces of the paths starting from τ_n and τ_{n-1} coincide, τ_n and τ_{n-1} have the same distance from the root, and such a distance is $\ell_n + 1$, by Claim 1

$$\tau_n \models_{M_n, Obs} \psi \Leftrightarrow \tau_{n-1} \models_{M_n, Obs} \psi$$



By applying Property 3 for the considered case, we have that

$$\tau_{n-1} \models_{K_n, Obs} \psi \Leftrightarrow \tau_{n-1} \models_{M_n, Obs} \psi$$

Hence, the result follows.

- Case $\psi : K_a \psi'$: Properties 1 and 2 directly follow from the induction hypothesis and the fact that for all $i \in [0, \ell_n]$, the two traces of $\pi[0, i]$ in K_n and M_n coincide. Now, we prove Property 3. If $p \in Obs(a)$, then since $i \geq \ell_n + 1$, by Remark A.1, $\pi(i + 1)$ is the unique node of K_n (resp., M_n) which is Obs_a -equivalent to $\pi(i + 1)$ itself. Hence, in this case, the result directly follows from the induction hypothesis.

Now, assume that $p \notin Obs(a)$. Hence, two nodes are Obs_a -equivalent if they have the same distance from the root. First, we consider the implication $\pi, i \models_{K_n, Obs} \psi \Rightarrow \pi, i \models_{M_n, Obs} \psi$. Assume that $\pi, i \models_{K_n, Obs} \psi$. Let π' be an initial path. We need to show that $\pi', i \models_{M_n, Obs} \psi$. Since $\pi, i \models_{K_n, Obs} \psi$, it holds that $\pi', i \models_{K_n, Obs} \psi'$. Thus, if π' does not visit ξ_n , then the result directly follows from the induction hypothesis on Property 3. Otherwise, since $i \geq \ell_n + 1$, by construction, in M_n , the traces of $\pi(\xi_n)[i, \infty]$ and $\pi(\xi_{n-1})[i, \infty]$ coincide. Thus, since $i \geq \ell_n + 1$, by Claim 1, $\pi(\xi_n), i \models_{M_n, Obs} \psi' \Leftrightarrow \pi(\xi_{n-1}), i \models_{M_n, Obs} \psi'$. Since $\pi(\xi_{n-1}), i \models_{K_n, Obs} \psi'$, by applying the induction hypothesis on Property 3, the result follows. The converse implication $\pi, i \models_{M_n, Obs} \psi \Rightarrow \pi, i \models_{K_n, Obs} \psi$ is similar, but we use the fact that in K_n , for each $i \geq \ell_n + 1$, the traces of $\pi(\xi_n)[i, \infty]$ and $\pi(\eta)[i, \infty]$ coincide. ◀

A.2 Proof of Theorem 12

In this Subsection, we prove the following result, where for the fixed $n > 1$, K_n and M_n are the regular tree structures over $2^{\{p\}}$ defined in Subsection 3.2.

► **Theorem 12.** *For all HyperCTL* sentences ψ such that $|\psi| < n$, $K_n \models \psi \Leftrightarrow M_n \models \psi$.*

In order to prove Theorem 12, first, we give some definitions and preliminary results which capture the recursive structure of K_n and M_n . In the following, for path assignment Π , we mean a path assignment of K_n . Since K_n and M_n coincide but for the labeling (in particular, the labeling of the path $\pi[\xi_1]$ at position i_{alert}), a path assignment of K_n is a path assignment of M_n as well, and vice versa.

For the nodes ξ_h and ξ_k with $h, k \in [1, n]$, we write $\xi_h \preceq \xi_k$ to mean that $h \leq k$. Recall that ℓ_n is the greatest main position and by construction, ℓ_n is a main p -position of type ξ_1 . For a main position i , $p(i)$ denotes the smallest main p -position j such that $j \geq i$. A main position which is not a p -main position is called a *main \emptyset -position*.

Fix $h_* \in [1, n]$ (representing node ξ_{h_*}).

► **Definition 27** (h_* -types and h_* -macro-blocks). Let i be a main p -position. The h_* -type of i is the type of i if either $h_* = 1$, or $i \neq i_{alert}$; otherwise, the h_* -type of i is ξ_{h_*} .

An h_* -macro-block bl is a set of main positions of the form $[i, j]$ such that $i < j$, i and j are main p -positions having the same h_* -type ξ_k , and there is no main p -position in $[i + 1, j - 1]$ with h_* -type $\xi_r \preceq \xi_k$.

A *pure macro-block* is a 1-macro-block. For an h_* -macro-block $bl = [i, j]$, the h_* -type of bl is the common h_* -type of i and j .

► **Remark.** For each main p -position i , there is at most one h_* -macro-block bl whose first position is i .

When $h_* \neq 1$, intuitively, the main p -position i_{alert} is “considered” a main p -position associated to the path $\pi(\xi_{h_*})$. More precisely, if we consider h_* -macro-blocks $bl = [i, j]$, where one bound is i_{alert} and the other one has type ξ_{h_*} (by construction, there are exactly two of such macro-blocks), then as we will prove, positions i and j are indistinguishable by HyperCTL^* formulas of size at most $n - 1$ which are evaluated on M_n with respect to path assignments where $\pi(\xi_{h_*})$ is not bound.

► **Definition 28** (h_* -low-ancestors and h_* -orders). Let i be a main p -position of h_* -type ξ_k . The h_* -low-ancestor of i is the smallest main p -position $j > i$ whose h_* -type ξ_r satisfies $\xi_r \prec \xi_k$, if such a position exists; otherwise the h_* -low-ancestor of i is undefined.

Let bl and bl' be two h_* -macro-blocks: bl' is the h_* -successor of bl if bl and bl' are of the forms $[i, j]$ and $[j, k]$, respectively. The h_* -order of bl is the length $\ell \geq 1$ of the maximal sequence bl_1, \dots, bl_ℓ of h_* -macro-blocks such that $bl_1 = bl$ and bl_k is the h_* -successor of bl_{k-1} for all $k \in [2, \ell]$. The h_* -order of a main p -position i is the h_* -order of the h_* -macro-block having i as first position if such a h_* -macro-block exists; otherwise, the h_* -order of i is 0.

► **Remark.** For a main p -position i , either the h_* -type of i is ξ_1 , or the h_* -low-ancestor of i is defined.

Now, for each $\mathbf{m} \in [0, n]$, we introduce the crucial notion of (h_*, \mathbf{m}) -compatibility between main positions. Intuitively, this notion allows to capture the properties which make two main positions indistinguishable from HyperCTL^* sentences of size at most \mathbf{m} when evaluated on K_n (resp., M_n) and in case $h_* = 1$ (resp., $h_* \neq 1$).

► **Definition 29** ((h_*, \mathbf{m}) -Compatibility). Let $\mathbf{m} \in [0, n]$. Two main p -positions i and j are (h_*, \mathbf{m}) -compatible if the following conditions are inductively satisfied, where $o(i)$ and $o(j)$ are the h_* -orders of i and j :

- i and j have the same h_* -type;
- either $o(i) = o(j)$, or $o(i) > \mathbf{m}$ and $o(j) > \mathbf{m}$;
- either the common h_* -type of i and j is ξ_1 , or the h_* -low-ancestors of i and j are (h_*, \mathbf{m}) -compatible.

Two main \emptyset -positions i and j are (h_*, \mathbf{m}) -compatible if the following holds:

- $p(i)$ and $p(j)$ are (h_*, \mathbf{m}) -compatible;
- either $p(i) - i = p(j) - j$, or $p(i) - i > \mathbf{m}$ and $p(j) - j > \mathbf{m}$.

We denote by $R(h_*, \mathbf{m})$ the binary relation over main positions defined as: $(i, j) \in R(h_*, \mathbf{m})$ iff either i and j are (h_*, \mathbf{m}) -compatible main p -positions, or i and j are (h_*, \mathbf{m}) -compatible main \emptyset -positions.

Two h_* -macro-blocks $[i, j]$ and $[i', j']$ are (h_*, \mathbf{m}) -compatible if $(i, i') \in R(h_*, \mathbf{m})$ and $(j, j') \in R(h_*, \mathbf{m})$.

► **Remark.** $R(h_*, \mathbf{m})$ is an equivalence relation.

The following two Propositions 30 and 31 capture some crucial properties of the equivalence relation $R(h_*, \mathbf{m})$. They are used in the next Lemma 32 to show that two (h_*, \mathbf{m}) -compatible main positions are indistinguishable from HyperCTL^* formulas of size at most \mathbf{m} when evaluated on the regular tree structure K_n whenever $h_* = 1$, and are indistinguishable from HyperCTL^* formulas of size at most \mathbf{m} when evaluated on the regular tree structure M_n whenever $h_* \neq 1$ and the initial path $\pi(\xi_{h_*})$ is not bound by the given path assignment.

► **Proposition 30.** Let $h_* \in [1, n]$, $\mathbf{m} \in [0, n]$, i_L and j_L be two main p -positions of h_* -type ξ_h such that $(i_L, j_L) \in R(h_*, \mathbf{m})$, and i_U and j_U be two main p -positions of h_* -type

ξ_k such that $i_U > i_L$, $j_U > j_L$ and $(i_U, j_U) \in R(h_*, \mathbf{m})$. If there is no main p -position in $[i_L + 1, i_U - 1] \cup [j_L + 1, j_U - 1]$ of h_* -type ξ_r such that $\xi_r \preceq \xi_h$ and $\xi_r \preceq \xi_k$, then, the following holds:

1. the restriction of $R(h_*, \mathbf{m})$ to $[i_L, i_U] \times [j_L, j_U]$ is total and $(i_L + 1, j_L + 1) \in R(h_*, \mathbf{m})$.⁴
2. for each $\wp \in [i_L, i_U - 1]$, there exists $\wp' \in [j_L, j_U - 1]$, such that $(\wp, \wp') \in R(h_*, \mathbf{m})$ and the restriction of $R(h_*, \mathbf{m})$ to $[i_L, \wp - 1] \times [j_L, \wp' - 1]$ is total.

Proof. We prove Properties 1 and 2 by induction on $2n - (h + k)$.

Base case: $2n - (h + k) = 0$. Hence, $k = h = n$. By hypothesis and construction, the sets $[i_L + 1, i_U - 1]$ and $[j_L + 1, j_U - 1]$ contain only main \emptyset -positions, and they have cardinality at least $n + 1$. Thus, since $\mathbf{m} \in [0, n]$, by definition of (h_*, \mathbf{m}) -compatibility, the result easily follows.

Base case: $2n - (h + k) > 0$. Let $\ell = \max(h, k)$. If $\ell = n$, by hypothesis $[i_L + 1, i_U - 1]$ and $[j_L + 1, j_U - 1]$ contain only main \emptyset -positions. Thus, by reasoning as in the base case, the result follows. Now, assume that $\ell < n$. Then, by hypothesis and construction, it follows that there must be $m_i, m_j > n + 3$ and $m_i + m_j$ h_* -macro-blocks of h_* -type $\xi_{\ell+1}$

$$bl_{m_i}^i, \dots, bl_1^i, bl_{m_j}^j, \dots, bl_1^j$$

such that the following holds, where f_i (resp., f_j) is the first position of $bl_{m_i}^i$ (resp., $bl_{m_j}^j$), and l_i (resp., l_j) is the last position of bl_1^i (resp., bl_1^j):

- for all $1 \leq r \leq m_i$, $bl_r^i \subseteq [i_L + 1, i_U - 1]$ and bl_r^i is the h_* -successor of bl_{r+1}^i if $r < m_i$.
- for all $1 \leq r \leq m_j$, $bl_r^j \subseteq [j_L + 1, j_U - 1]$ and bl_r^j is the h_* -successor of bl_{r+1}^j if $r < m_j$.
- There is no main p -position in $[i_L + 1, f_i - 1] \cup [j_L + 1, f_j - 1] \cup [l_i + 1, i_U - 1] \cup [l_j + 1, j_U - 1]$ of h_* -type ξ_r such that $\xi_r \preceq \xi_{\ell+1}$.

Hence, we also deduce that (recall that $\mathbf{m} \in [0, n]$).

- $(f_i, f_j) \in R(h_*, \mathbf{m})$ and $(l_i, l_j) \in R(h_*, \mathbf{m})$;
- for all $1 \leq r \leq n + 1$, bl_r^i and bl_r^j are (h_*, \mathbf{m}) -compatible h_* -macro-blocks;
- for all $n + 1 < r \leq m_i$ and $n + 1 < s \leq m_j$, bl_r^i and bl_s^j are (h_*, \mathbf{m}) -compatible h_* -macro-blocks.

Since $\ell + 1 \geq \max(h, k) + 1$, by applying the induction on Property 1, we obtain that:

- (I) the restriction of $R(h_*, \mathbf{m})$ to $[i_L, f_i] \times [j_L, f_j]$ is total and $(i_L + 1, j_L + 1) \in R(h_*, \mathbf{m})$;
- (II) the restriction of $R(h_*, \mathbf{m})$ to $[l_i, i_U] \times [l_j, j_U]$ is total;
- (III) for all $1 \leq r \leq n + 1$, the restriction of $R(h_*, \mathbf{m})$ to $bl_r^i \times bl_r^j$ is total;
- (IV) for all $n + 1 < r \leq m_i$ and $n + 1 < s \leq m_j$, the restriction of $R(h_*, \mathbf{m})$ to $bl_r^i \times bl_s^j$ is total.

Hence, since $m_i > n + 3$ and $m_j > n + 3$, Property 1 follows. Now, we prove Property 2. We distinguish, four cases:

- $\wp \in [i_L, f_i - 1]$. Recall that $(f_i, f_j) \in R(h_*, \mathbf{m})$, f_i and f_j have h_* -type $\xi_{\ell+1}$, and there is no main p -position in $[i_L + 1, f_i - 1] \cup [j_L + 1, f_j - 1]$ of type ξ_r such that $\xi_r \preceq \xi_{\ell+1}$. Thus, since $\ell = \max(h, k)$, we can apply the induction hypothesis on Property 2, and the result follows.
- $\wp \in [l_i, i_U - 1]$. This case is similar to the previous one.

⁴ Recall that a binary relation $R \subseteq S \times S'$ is total if for all $s \in S$ (resp., $s \in S'$), there is $s' \in S'$ (resp., $s \in S$) such that $(s, s') \in R$.

- there is $1 \leq r \leq n+1$ such that $\wp \in bl_r^i$ and \wp is *not* the last position of bl_r^i . Let $bl_r^i = [f_r^i, l_r^i]$ and $bl_r^j = [f_r^j, l_r^j]$. Recall that bl_r^i and bl_r^j are (h_*, \mathbf{m}) -compatible h_* -macro-blocks of h_* -type $\xi_{\ell+1}$. Hence, $(f_r^i, f_r^j), (l_r^i, l_r^j) \in R(h_*, \mathbf{m})$, $f_r^i, f_r^j, l_r^i, l_r^j$ have h_* -type $\xi_{\ell+1}$, and there is no main p -position in $[f_r^i+1, l_r^i-1] \cup [f_r^j+1, l_r^j-1]$ of type ξ_r such that $\xi_r \preceq \xi_{\ell+1}$. Moreover, by Conditions (I), (III) and (IV) above, the restriction of $R(h_*, \mathbf{m})$ to $[i_L, f_r^i] \times [j_L, f_r^j]$ is total. Thus, since $\wp \in [f_r^i, l_r^i-1]$, by applying the induction hypothesis on Property 2, the result follows.
- there is $n+1 < r \leq m_i$ such that $\wp \in bl_r^i$ and \wp is *not* the last position of bl_r^i . Recall that for all $n+1 < s \leq m_j$, bl_r^i and bl_s^j are (h_*, \mathbf{m}) -compatible h_* -macro-blocks of h_* -type $\xi_{\ell+1}$. Choice $n+1 < s \leq m_j$ such that $s = m_j$ iff $r = m_i$. Note that such a s exists since $m_j > n+3$. Let $bl_r^i = [f_r^i, l_r^i]$ and $bl_s^j = [f_s^j, l_s^j]$. By Conditions (I), (III) and (IV) above, the restriction of $R(h_*, \mathbf{m})$ to $[i_L, f_r^i] \times [j_L, f_s^j]$ is total. Since $\wp \in [f_r^i, l_r^i-1]$, by reasoning as in the previous case, Property 2 follows. ◀

► **Proposition 31.** *Let $h_* \in [1, n]$, $\mathbf{m} \in [1, n]$, $(\ell, \ell') \in R(h_*, \mathbf{m})$, and \wp be a main position such that $\wp \geq \ell$. Then, the following holds:*

1. *either $\ell = \ell'$ or $(\ell+1, \ell'+1) \in R(h_*, \mathbf{m}-1)$;*
2. *there is a main position $\wp' \geq \ell'$ such that $(\wp, \wp') \in R(h_*, \mathbf{m}-1)$ and the restriction of $R(h_*, \mathbf{m}-1)$ to $[\ell, \wp-1] \times [\ell', \wp'-1]$ is total.*

Proof. Let $h_* \in [1, n]$, $\mathbf{m} \in [1, n]$, $(\ell, \ell') \in R(h_*, \mathbf{m})$ and \wp be a main position such that $\wp \geq \ell$. Recall that ℓ_n is the greatest main position. Moreover, by construction, ℓ_n is a main p -position having h_* -type ξ_1 and h_* -order 0.

We prove Properties 1 and 2 by induction on $\ell_n - \ell$. For the base case, $\ell_n - \ell = 0$. Since $(\ell, \ell') \in R(h_*, \mathbf{m})$, by definition of (h_*, \mathbf{m}) -compatibility, $\ell_n - \ell' = 0$ as well. Hence, Properties 1 and 2 follows.

For the induction step, assume that $\ell_n - \ell > 0$. Hence, $\ell_n - \ell' > 0$ as well. First, we consider the case when ℓ is a main p -position (hence, ℓ' is a main p -position as well). If $\ell = \ell'$, Properties 1 and 2 trivially hold. Now, assume that $\ell \neq \ell'$. Let $o(\ell)$ and $o(\ell')$ be the h_* -orders of ℓ and ℓ' . We distinguish two cases:

- $o(\ell) = 0$: since $(\ell, \ell') \in R(h_*, \mathbf{m})$, it holds that $o(\ell') = 0$. Note that ℓ_n is the unique main p -position having h_* -type ξ_1 and h_* -order 0. Thus, since $\ell \neq \ell_n$, $\ell' \neq \ell_n$, and $(\ell, \ell') \in R(h_*, \mathbf{m})$, the h_* -low-ancestors $a(\ell)$ and $a(\ell')$ of ℓ and ℓ' are defined and $(a(\ell), a(\ell')) \in R(h_*, \mathbf{m})$. Moreover, denoting ξ_h (resp., ξ_k) the common h_* -type of ℓ and ℓ' (resp., $a(\ell)$ and $a(\ell')$), there is no main p -position in $[\ell, a(\ell)] \cup [\ell', a(\ell')]$ having h_* -type ξ_r such that $\xi_r \preceq \xi_h$ and $\xi_r \preceq \xi_k$. Hence, by Proposition 30(1), $(\ell+1, \ell'+1) \in R(h_*, \mathbf{m})$. Thus, since $R(h_*, \mathbf{m}) \subseteq R(h_*, \mathbf{m}-1)$, Property 1 follows. Now, we prove Property 2. We distinguish two cases:
 - $\wp \in [\ell, a(\ell)-1]$. By applying Proposition 30(2), there exists $\wp' \in [\ell', a(\ell')-1]$ such that $(\wp, \wp') \in R(h_*, \mathbf{m})$ and the restriction of $R(h_*, \mathbf{m})$ to $[\ell, \wp-1] \times [\ell', \wp'-1]$ is total. Thus, since $R(h_*, \mathbf{m}-1) \supseteq R(h_*, \mathbf{m})$, Property 2 follows.
 - $\wp \geq a(\ell)$. Since $R(h_*, \mathbf{m}-1) \supseteq R(h_*, \mathbf{m})$, by applying Proposition 30(1), the restriction of $R(h_*, \mathbf{m}-1)$ to $[\ell, a(\wp)] \times [\ell', a(\wp)]$ is total. Thus, since $(a(\ell), a(\ell')) \in R(h_*, \mathbf{m})$, $\wp \geq a(\ell)$ and $a(\ell) > \ell$, by applying the induction hypothesis, Property 2 follows.
- $o(\ell) > 0$: since $(\ell, \ell') \in R(h_*, \mathbf{m})$, it holds that $o(\ell') > 0$. Hence, there exist two h_* -macro-blocks of the form $bl = [\ell, i_U]$ and $bl' = [\ell', i'_U]$. Let $o(i_U)$ and $o(i'_U)$ be the h_* -orders of i_U and i'_U . Note that $o(i_U) = o(\ell) - 1$ and $o(i'_U) = o(\ell') - 1$. Since $(\ell, \ell') \in R(h_*, \mathbf{m})$, either $o(\ell) = o(\ell')$, or $o(\ell), o(\ell') > \mathbf{m}$. Hence, only the following two cases are possible:

- $o(i_U) = o(i'_U)$, or $o(i_U), o(i'_U) > \mathbf{m}$. Since the h_* -low-ancestor of i_U (resp., i'_U) coincides with the h_* -low-ancestor of ℓ (resp., ℓ'), we have that $(i_U, i'_U) \in R(h_*, \mathbf{m})$. By reasoning as for the case $o(\ell) = 0$ (we just replace $a(\ell)$ and $a(\ell')$ with i_U and i'_U , respectively), Property 1 and 2 follow.
- there exists $k \geq 1$ such that $\{o(i_U), o(i'_U)\} = \{\mathbf{m}, \mathbf{m} + k\}$. It follows that $(i_U, i'_U) \in R(h_*, \mathbf{m} - 1)$. Since $(\ell, \ell') \in R(h_*, \mathbf{m})$, $(\ell, \ell') \in R(h_*, \mathbf{m} - 1)$. Thus, by applying Proposition 30(1), we obtain that $(\ell + 1, \ell' + 1) \in R(h_*, \mathbf{m} - 1)$, and Property 1 follows. Now, we prove Property 2. First, assume that $\wp \in [\ell, i_U - 1]$. Applying Proposition 30(2), there exists $\wp' \in [\ell', i'_U - 1]$ such that $(\wp, \wp') \in R(h_*, \mathbf{m} - 1)$ and the restriction of $R(h_*, \mathbf{m} - 1)$ to $[\ell, \wp - 1] \times [\ell', \wp' - 1]$ is total. Hence, Property 2 follows.

Now, assume that $\wp \geq i_U$. By hypothesis, $\{o(i_U), o(i'_U)\} = \{\mathbf{m}, \mathbf{m} + k\}$ for some $k \geq 1$. Assume that $o(i_U) = \mathbf{m}$ and $o(i'_U) = \mathbf{m} + k$ (the other case being similar). Additionally, for simplicity, we also assume that $k = 1$ (the general case can be handled in a similar way). Let $bl'' = (i'_U, i''_U)$ be the h_* -macro-block which is the h_* -successor of bl' (note that bl'' exists since $o(i'_U) = \mathbf{m} + 1$). Then, the h_* -order $o(i''_U)$ of i''_U is \mathbf{m} and $(i_U, i''_U) \in R(h_*, \mathbf{m})$, hence, $(i_U, i''_U) \in R(h_*, \mathbf{m} - 1)$ as well. Since $(i_U, i'_U) \in R(h_*, \mathbf{m} - 1)$, by Proposition 30(1), the restriction of $R(h_*, \mathbf{m} - 1)$ to $bl \times bl'$ (resp., $bl \times bl''$) is total. Hence, the restriction of $R(h_*, \mathbf{m} - 1)$ to $[\ell, i_U] \times [\ell', i''_U]$ is total. Thus, since $(i_U, i''_U) \in R(h_*, \mathbf{m})$, $\wp \geq i_U$ and $i_U > \ell$, by applying the induction hypothesis, the result follows.

It remains to consider the case when ℓ is a \emptyset -main position. Since $(\ell, \ell') \in R(h_*, \mathbf{m})$, ℓ' is a main \emptyset -position as well. Moreover, $(p(\ell), p(\ell')) \in R(h_*, \mathbf{m})$ and either $p(\ell) - \ell = p(\ell') - \ell'$, or $p(\ell) - \ell > \mathbf{m}$ and $p(\ell') - \ell' > \mathbf{m}$. Thus, since we have already proved that Properties 1 and 2 hold when ℓ is a main p -position, by applying the induction hypothesis to the main p -position $p(\ell)$, the result easily follows. \blacktriangleleft

► **Lemma 32.** *Let $h_* \in [1, n]$, ψ be an HyperCTL* formula such that $|\psi| \leq n$, and $(\ell, \ell') \in R(h_*, |\psi|)$.*

1. *If $h_* = 1$, then for all path assignments Π and $x \in \text{VAR}$,*

$$\Pi, x, \ell \models_{K_n} \psi \Leftrightarrow \Pi, x, \ell' \models_{K_n} \psi$$

2. *If $h_* \in [2, n]$, then for all path assignments Π such that $\pi(\xi_{h_*})$ is not bound by Π , and $x \in \text{VAR}$*

$$\Pi, x, \ell \models_{M_n} \psi \Leftrightarrow \Pi, x, \ell' \models_{M_n} \psi$$

Proof. We prove Property 2 (Property 1 being similar). Let $h_* \in [2, n]$, ψ be an HyperCTL* formula such that $|\psi| \leq n$, and Π be an assignment path such that $\pi(\xi_{h_*})$ is not bound by Π . We need to prove that for all $x \in \text{VAR}$ and $(\ell, \ell') \in R(h_*, |\psi|)$,

$$\Pi, x, \ell \models_{M_n} \psi \Leftrightarrow \Pi, x, \ell' \models_{M_n} \psi$$

The proof is by induction on $|\psi|$. The cases for the boolean connectives \neg and \wedge directly follow from the inductive hypothesis and the fact that $R(h_*, \mathbf{m}) \subseteq R(h_*, \mathbf{m}')$ for all $\mathbf{m}, \mathbf{m}' \in [0, n]$ such that $\mathbf{m} \geq \mathbf{m}'$. For the other cases, we proceed as follows.

- Case $\psi = p'[y]$ for some $p' \in \text{AP}$ and $y \in \text{VAR}$: we show that the labels of $\Pi(y)(\ell)$ and $\Pi(y)(\ell')$ in M_n coincide. Since $(\ell, \ell') \in R(h_*, |\psi|)$, either ℓ and ℓ' are both main \emptyset -positions, or ℓ and ℓ' are both main p -positions.

If $\Pi(y)$ is the initial path visiting node η (i.e., $\Pi(y) = \pi(\eta)$), then by construction, $\Pi(y)(\ell)$ and $\Pi(y)(\ell')$ have the same label in M_n , and the result follows. Otherwise, $\Pi(y) = \pi(\xi_k)$ for some $k \in [1, n]$. If ℓ and ℓ' are main \emptyset -positions, then by construction, $\Pi(y)(\ell)$ and $\Pi(y)(\ell')$ have both empty label in M_n , and the result follows. Now, assume that ℓ and ℓ' are main p -positions. By hypothesis, $k \neq h_*$ and $h_* \in [2, n]$. Since $(\ell, \ell') \in R(h_*, |\psi|)$, by construction, *either* ℓ and ℓ' have the same type ξ_h and $\ell, \ell' \neq i_{alert}$, *or* $\ell = i_{alert}$ (resp., $\ell' = i_{alert}$) and ℓ' has type ξ_{h_*} (resp., ℓ has type ξ_{h_*}). Thus, since $k \neq h_*$, by construction of M_n , the result follows.

- Case $\psi = X\psi'$. Since $(\ell, \ell') \in R(h_*, |\psi|)$ and $|\psi'| = |\psi| - 1$, by Proposition 31(1), either $\ell = \ell'$, or $(\ell + 1, \ell' + 1) \in R(h_*, |\psi'|)$. In the first case, the result trivially follows. In the second case, since $(\ell + 1, \ell' + 1) \in R(h_*, |\psi'|)$, by applying the induction hypothesis, we have

$$\Pi, x, \ell + 1 \models_{M_n} \psi' \Leftrightarrow \Pi, x, \ell' + 1 \models_{M_n} \psi'$$

Hence, the result follows.

- $\psi = \psi_1 \cup \psi_2$: we prove the direction $\Pi, x, \ell \models_{M_n} \psi \Rightarrow \Pi, x, \ell' \models_{M_n} \psi$ (the converse direction being symmetric). Let $\Pi, x, \ell \models_{M_n} \psi$. By hypothesis, there exists $\wp \geq \ell$ such that $\Pi, x, \wp \models_{M_n} \psi_2$ and $\Pi, x, i \models_{M_n} \psi_1$ for all $i \in [\ell, \wp - 1]$. We will prove that $\Pi, x, \ell' \models_{M_n} \psi$. We distinguish two cases:
 - \wp is a main position. Since $(\ell, \ell') \in R(h_*, |\psi|)$, by applying Proposition 31(2), there exists $\wp' \geq \ell'$ such that $(\wp, \wp') \in R(h_*, |\psi| - 1)$ and the restriction of $R(h_*, |\psi| - 1)$ to $[\ell, \wp - 1] \times [\ell', \wp' - 1]$ is total. Since $R(h_*, |\psi| - 1) \subseteq R(h_*, |\psi_2|)$, $(\wp, \wp') \in R(h_*, |\psi| - 1)$, and $\Pi, x, \wp \models_{M_n} \psi_2$, by applying the induction hypothesis, we obtain that $\Pi, x, \wp' \models_{M_n} \psi_2$. Moreover, since $R(h_*, |\psi| - 1) \subseteq R(h_*, |\psi_1|)$, $\Pi, x, i \models_{M_n} \psi_1$ for all $i \in [\ell, \wp - 1]$, and the restriction of $R(h_*, |\psi| - 1)$ to $[\ell, \wp - 1] \times [\ell', \wp' - 1]$ is total, by applying the induction hypothesis, we obtain that $\Pi, x, i \models_{M_n} \psi_1$ for all $i \in [\ell', \wp' - 1]$. Hence, $\Pi, x, \ell' \models_{M_n} \psi$ and the result follows.
 - \wp is not a main position. Hence, $\wp > \ell_n$ and $\Pi, x, \ell_n \models_{M_n} \psi$ (recall that ℓ_n is the greatest main position). By applying Proposition 31(2), there exists $j \geq \ell'$ such that $(\ell_n, j) \in R(h_*, |\psi| - 1)$ and the restriction of $R(h_*, |\psi| - 1)$ to $[\ell, \ell_n] \times [\ell', j]$ is total. Since $|\psi| - 1 \geq 1$ and $(\ell_n, j) \in R(h_*, |\psi| - 1)$, by Proposition 31(1), either $(\ell_n + 1, j + 1) \in R(h_*, |\psi| - 1)$ or $j = \ell_n$. Since ℓ_n is the greatest main position, we deduce that $j = \ell_n$. Hence, since $R(h_*, |\psi| - 1) \subseteq R(h_*, |\psi_1|)$ and $\Pi, x, i \models_{M_n} \psi_1$ for all $i \in [\ell, \ell_n]$, by applying the induction hypothesis, we have that $\Pi, x, i \models_{M_n} \psi_1$ for all $i \in [\ell', \ell_n]$. Thus, since $\Pi, x, \ell_n \models_{M_n} \psi$, the result follows.
- $\psi = \exists y. \psi'$. Since ℓ and ℓ' are main positions, $\ell, \ell' > 0$. By construction, for each initial path π of M_n and for each position $i > 0$, π is the unique path having $\pi[0, i]$ as a prefix. Hence, for all $i \in \{\ell, \ell'\}$, $\Pi, x, i \models_{M_n} \psi \Leftrightarrow \Pi, x, i \models_{M_n} \psi'$. Hence, the result directly follows from the induction hypothesis.

◀

Now, we prove the crucial lemma from which Theorem 12 directly follows. Let bl_{alert} be the pure macro-block of type t_1 whose last position is i_{alert} . The size $|\Pi|$ of a path assignment is the number of initial paths of K_n (or equivalently, M_n) which are bound by Π .

► **Lemma 33.** *Let ψ be an HyperCTL* formula and Π be a path assignment such that $|\Pi| + |\psi| < n$. Moreover, let i_F be the first position of bl_{alert} . Then, for all $\ell \leq i_F$ and*

$x \in \text{VAR}$,

$$\Pi, x, \ell \models_{K_n} \psi \Leftrightarrow \Pi, x, \ell \models_{M_n} \psi$$

Proof. Let ψ , Π , i_F , x and ℓ as in the statement of the lemma. First, we make some crucial observations. The first one (Claim 1) directly follows from construction and the semantics of HyperCTL*.

Claim 1: for all $\ell > i_{\text{alert}}$, $\Pi, x, \ell \models_{K_n} \psi \Leftrightarrow \Pi, x, \ell \models_{M_n} \psi$

Moreover, since $|\Pi| < n - 1$, there must be h_* such that

Claim 2: $h_* \in [2, n]$ and the path $\pi(t_{h_*})$ is not bound by Π .

Let i_N be the fourth (in increasing order) main p -position of type t_1 . Since i_{alert} is the third (in increasing order) main p -position of type 1, by construction, the 1-order and the h_* -order of i_N are both n . Hence, by definition of $(1, n - 1)$ -compatibility and $(h_*, n - 1)$ -compatibility, the following holds.

Claim 3: $(1, i_F) \in R(1, n - 1)$, $(i_F, i_{\text{alert}}) \in R(1, n - 1)$, and $(i_{\text{alert}}, i_N) \in R(1, n - 1)$. Moreover, $(1, i_F) \in R(h_*, n - 1)$ and $(i_F, i_N) \in R(h_*, n - 1)$.

Now, we prove the lemma by induction on $|\psi|$. The cases for the boolean connectives directly follows from the induction hypothesis. For the other cases, we proceed as follows.

- $\psi = p'[y]$ for some $p' \in \text{AP}$ and $y \in \text{VAR}$: by hypothesis $\ell \leq i_F$ and $i_F < i_{\text{alert}}$. By construction, it follows that the labels of $\Pi(y)(\ell)$ in K_n and M_n coincide. Hence, the result follows.
- $\psi = X\psi'$. If $\ell < i_F$, we apply the induction hypothesis on ψ' with respect to position $\ell + 1 \leq i_F$, and the result follows.
Now, assume that $\ell = i_F$. By Claim 3, $(1, i_F) \in R(1, n - 1)$. Moreover, since $|\psi| < n$, $R(1, n - 1) \subseteq R(1, |\psi|)$. Thus, by Lemma 32(1), we have that

$$\Pi, x, 1 \models_{K_n} \psi \Leftrightarrow \Pi, x, i_F \models_{K_n} \psi$$

By Claim 2 and 3, $(1, i_F) \in R(h_*, n - 1)$, $h_* \in [2, n]$, and $\pi(\xi_{h_*})$ is not bound by the path assignment Π . Since, $R(h_*, n - 1) \subseteq R(h_*, |\psi|)$, by Lemma 32(1), we have

$$\Pi, x, 1 \models_{M_n} \psi \Leftrightarrow \Pi, x, i_F \models_{M_n} \psi$$

Thus, since $\psi = X\psi'$, by applying the induction hypothesis on ψ' with respect to position $2 \leq i_F$, the result follows.

- $\psi = \psi_1 U \psi_2$. By applying the induction hypothesis on ψ_1 and ψ_2 and by the semantics of the until modality, it suffices to show that

$$\Pi, x, i_F \models_{K_n} \psi \Leftrightarrow \Pi, x, i_F \models_{M_n} \psi$$

By Claim 3, $(i_F, i_{\text{alert}}) \in R(1, n - 1)$ and $(i_{\text{alert}}, i_N) \in R(1, n - 1)$. Moreover, since $|\psi| < n - 1$, $R(1, n - 1) \subseteq R(1, |\psi|)$. Thus, by applying twice Lemma 32(1), we obtain

$$\Pi, x, i_F \models_{K_n} \psi \Leftrightarrow \Pi, x, i_N \models_{K_n} \psi$$

By Claim 2 and 3, $(i_F, i_N) \in R(h_*, n - 1)$, $h_* \in [2, n]$, and $\pi(\xi_{h_*})$ is not bound by the path assignment Π . Since, $R(h_*, n - 1) \subseteq R(h_*, |\psi|)$, by applying Lemma 32(2), we obtain

$$\Pi, x, i_F \models_{M_n} \psi \Leftrightarrow \Pi, x, i_N \models_{M_n} \psi$$

Since $i_N > i_{alert}$, by Claim 1,

$$\Pi, x, i_N \models_{K_n} \psi \Leftrightarrow \Pi, x, i_N \models_{M_n} \psi$$

Hence, the result follows.

- $\psi = \exists y.\psi'$. By hypothesis $|\Pi| + |\psi| < n$. Hence, for each initial path π of K_n (or equivalently M_n) and for each $y \in \text{VAR}$, $|\Pi[y \leftarrow \pi]| + |\psi'| < n$. By applying the induction hypothesis, we have that $\Pi[y \leftarrow \pi], y, \ell \models_{K_n} \psi' \Leftrightarrow \Pi[y \leftarrow \pi], y, \ell \models_{M_n} \psi'$. Hence, $\Pi, x, \ell \models_{K_n} \psi \Leftrightarrow \Pi, x, \ell \models_{M_n} \psi$, and the result follows. ◀

A.3 Proof of Theorem 13

► **Theorem 13.** *Given a KCTL* sentence ψ and an observation map Obs , one can construct in linear time a HyperCTL*_{lp} sentence φ with just two path variables such that for each Kripke structure K , $K \models \varphi \Leftrightarrow (K, Obs) \models \psi$.*

Proof. Let $x_0, x_1 \in \text{VAR}$ with $x_0 \neq x_1$ and Obs be an observation map. We inductively define a mapping $f_{Obs} : \text{KCTL}^* \times \{0, 1\} \rightarrow \text{HyperCTL}^*_{lp}$ as follows, where $h \in \{0, 1\}$:

- $f_{Obs}(\top, h) = \top$
- $f_{Obs}(p, h) = p[x_h]$ for all $p \in \text{AP}$;
- $f_{Obs}(\neg\psi, h) = \neg f_{Obs}(\psi, h)$;
- $f_{Obs}(\psi_1 \wedge \psi_2, h) = f_{Obs}(\psi_1, h) \wedge f_{Obs}(\psi_2, h)$;
- $f_{Obs}(\mathbf{X}\psi, h) = \mathbf{X}f_{Obs}(\psi, h)$;
- $f_{Obs}(\psi_1 \mathbf{U} \psi_2, h) = f_{Obs}(\psi_1, h) \mathbf{U} f_{Obs}(\psi_2, h)$;
- $f_{Obs}(\exists\psi, h) = \exists x_h.f_{Obs}(\psi, h)$;
- $f_{Obs}(K_a\psi, h) = \forall^G x_{1-h}. \left(\left(G^- \bigwedge_{p \in Obs(a)} (p[x_h] \leftrightarrow p[x_{h-1}]) \right) \longrightarrow f_{Obs}(\psi, x_{1-h}) \right)$.

By construction, for all $h = 1, 2$ and KCTL* sentences ψ , $f_{Obs}(\psi, h)$ is a HyperCTL*_{lp} sentence of size linear in $|\psi|$. Thus, Theorem 13 directly follows from the following claim.

Claim: let $K = \langle S, s_0, E, V \rangle$ be a Kripke structure and π be an initial path of K . Then, for all KCTL* formulas ψ , $h = 0, 1$, $i \geq 0$, and path assignment Π such that $\Pi(x_h) = \pi$, the following holds:

$$\Pi, x_h, i \models_K f_{Obs}(\psi, h) \Leftrightarrow \pi, i \models_{(K, Obs)} \psi$$

Proof of the claim: the proof is by induction on $|\psi|$.

- $\psi = \top$: trivial;
- $\psi = p$ with $p \in \text{AP}$: by construction, $f_{Obs}(p, h) = p[x_h]$. Thus, since $\Pi(x_h) = \pi$, the result follows.
- $\psi = \neg\psi'$ or $\psi = \psi_1 \wedge \psi_2$ or $\psi = \mathbf{X}\psi'$ or $\psi = \psi_1 \mathbf{U} \psi_2$: by construction, the result directly follows from the induction hypothesis.
- $\psi = \exists\psi'$: then, $\Pi, x_h, i \models_K f_{Obs}(\psi, h) \Leftrightarrow$ (by construction) $\Pi, x_h, i \models_K \exists x_h.f_{Obs}(\psi', h) \Leftrightarrow$ (by the semantics of HyperCTL*_{lp}) there exists an initial path π' of K such that $\pi'[0, i] = \Pi(x_h)[0, i]$ and $\Pi[x_h \leftarrow \pi'], x_h, i \models_K f_{Obs}(\psi', h) \Leftrightarrow$ (by the induction hypothesis and since $\Pi(x_h) = \pi$) there exists an initial path π' of K such that $\pi'[0, i] = \pi[0, i]$ and $\pi', i \models_{(K, Obs)} \psi' \Leftrightarrow$ (by the semantics of KCTL*) $\pi, i \models_{(K, Obs)} \psi$. Hence, the result follows.

- $\psi = K_a\psi'$: then, $\Pi, x_h, i \models_K f_{Obs}(K_a\psi, h) \Leftrightarrow$ (by construction and the semantics of HyperCTL_{lp}^*) for all initial paths π' of K ,

$$\Pi[x_{1-h} \leftarrow \pi'], x_{1-h}, i \models_K (\mathbf{G}^- \bigwedge_{p \in Obs(a)} (p[x_h] \leftrightarrow p[x_{h-1}])) \longrightarrow f_{Obs}(\psi', x_{1-h})$$

\Leftrightarrow (since $\Pi[x_{1-h} \leftarrow \pi'](x_h) = \Pi(x_h) = \pi$ for all initial paths π' of K such that $V(\pi'[0, i])$ and $V(\pi[0, i])$ are Obs_a -equivalent, $\Pi[x_{1-h} \leftarrow \pi'], x_{1-h}, i \models_K f_{Obs}(\psi', x_{1-h}) \Leftrightarrow$ (by the induction hypothesis) for all initial paths π' of K such that $V(\pi'[0, i])$ and $V(\pi[0, i])$ are Obs_a -equivalent, $\pi', i \models_{(K, Obs)} \psi' \Leftrightarrow$ (by the semantics of KCTL^*) $\pi, i \models_{(K, Obs)} K_a\psi'$. Hence, the result follows. ◀

B

 Proofs from Section 4

B.1 Formal definitions of Büchi SNWA and two-way HAA

Büchi SNWA. A Büchi SNWA over an input alphabet Σ is a tuple $\mathcal{A} = \langle Q, Q_0, \rho, F_-, F_+ \rangle$, where Q is a finite set of states, $Q_0 \subseteq Q$ is a set of initial states, $\rho : Q \times \{\rightarrow, \leftarrow\} \times \Sigma \rightarrow 2^Q$ is a transition function, and F_- and F_+ are sets of accepting states. Intuitively, the symbols \rightarrow and \leftarrow are used to denote forward and backward moves. A run of \mathcal{A} over a pointed word (w, i) is a pair $r = (r_{\leftarrow}, r_{\rightarrow})$ such that $r_{\rightarrow} = q_i, q_{i+1} \dots$ is an infinite sequence of states, $r_{\leftarrow} = p_i, p_{i-1} \dots p_0 p_{-1}$ is a finite sequence of states, and: (i) $q_i = p_i \in Q_0$; (ii) for each $h \geq i$, $q_{h+1} \in \rho(q_h, \rightarrow, w(h))$; and (iii) for each $h \in [0, i]$, $p_{h-1} \in \rho(p_h, \leftarrow, w(h))$.

Thus, starting from the initial position i in the input pointed word (w, i) , the automaton splits in two copies: the first one moves forwardly along the suffix of w starting from position i and the second one moves backwardly along the prefix $w(0) \dots w(i)$. The run $r = (r_{\leftarrow}, r_{\rightarrow})$ is *accepting* if $p_{-1} \in F_-$ and r_{\rightarrow} visits infinitely often some state in F_+ . A pointed word (w, i) is accepted by \mathcal{A} if there is an accepting run of \mathcal{A} over (w, i) . We denote by $\mathcal{L}_p(\mathcal{A})$ the set of pointed words accepted by \mathcal{A} and by $\mathcal{L}(\mathcal{A})$ the set of infinite words w such that $(w, 0) \in \mathcal{L}_p(\mathcal{A})$.

Two-way HAA. For a set X , $\mathcal{B}^+(X)$ denotes the set of positive Boolean formulas over X built from elements in X using \vee and \wedge (we also allow the formulas **true** and **false**). For a formula $\theta \in \mathcal{B}^+(X)$, a *model* Y of θ is a subset Y of X which satisfies θ . The model Y of θ is minimal if no strict subset of Y satisfies θ .

A two-way HAA \mathcal{A} over an alphabet Σ is a tuple $\mathcal{A} = \langle Q, q_0, \delta, F_-, F \rangle$, where Q is a finite set of states, $q_0 \in Q$ is the initial state, $\delta : Q \times \Sigma \rightarrow \mathcal{B}^+(\{\rightarrow, \leftarrow\} \times Q)$ is a transition function, $F_- \subseteq Q$ is the *backward acceptance condition*, and F is a *strata family* encoding a particular kind of parity acceptance condition and imposing some syntactical constraints on the transition function δ . Before defining F , we give the notion of run which is independent of F and F_- . We restrict ourselves to *memoryless* runs, in which the behavior of the automaton depends only on the current input position and current state. Since later we will deal only with parity acceptance conditions, memoryless runs are sufficient (see e.g. [4]).⁵ Formally, given a pointed word (w, i) on Σ and a state $p \in Q$, a (i, p) -run of \mathcal{A} over w is a directed graph $\langle V, E, v_0 \rangle$ with set of vertices $V \subseteq (\mathbb{N} \cup \{-1\}) \times Q$ and initial vertex $v_0 = (i, p)$. Intuitively, a vertex (j, q) describes a copy of the automaton which is in state q and reads the j^{th} input position. Additionally, we require that the set of edges E is consistent with the transition function δ . Formally, for every vertex $v = (j, q) \in V$ such that $j \geq 0$, there is a *minimal* model $\{(dir_1, q_1), \dots, (dir_n, q_n)\}$ of $\delta(q, w(j))$ such that the set of successors of $v = (j, q)$ is $\{(j_1, q_1), \dots, (j_n, q_n)\}$ and for all $k \in [1, n]$, $j_k = j + 1$ if $dir_k = \rightarrow$, and $j_k = j - 1$ otherwise.

An infinite path π of a run is *eventually strictly-forward* whenever π has a suffix of the form $(i, q_1), (i + 1, q_2), \dots$ for some $i \geq 0$.

Now, we formally define F and give the semantic notion of acceptance. F is a *strata family* of the form $F = \{\langle \rho_1, Q_1, F_1 \rangle, \dots, \langle \rho_k, Q_k, F_k \rangle\}$, where Q_1, \dots, Q_k is a partition of the set of states Q of \mathcal{A} , and for all $i \in [1, k]$, $\rho_i \in \{-, \mathbf{t}, \mathbf{B}, \mathbf{C}\}$ and $F_i \subseteq Q_i$, such that $F_i = \emptyset$ whenever $\rho_i \in \{\mathbf{t}, -\}$. A stratum $\langle \rho_i, Q_i, F_i \rangle$ is called a *negative* stratum if $\rho_i = -$, a *transient* stratum if $\rho_i = \mathbf{t}$, a Büchi stratum (with Büchi acceptance condition F_i) if $\rho_i = \mathbf{B}$, and a coBüchi stratum (with coBüchi acceptance condition F_i) if $\rho_i = \mathbf{C}$. Additionally, there

⁵ See references for the Appendix.

is a partial order \leq on the sets Q_1, \dots, Q_k such that the following holds:

- R1. Moves from states in Q_i lead to states in components Q_j such that $Q_j \leq Q_i$; additionally, if Q_i belongs to a transient stratum, there are no moves from Q_i leading to Q_i .
 - R2. For all moves (dir, q') from states $q \in Q_i$ such that $q' \in Q_i$ as well, the following holds: $dir \in \{\leftarrow\}$ if the stratum of Q_i is negative, and $dir \in \{\rightarrow\}$ otherwise.
- R1 is the *stratum order requirement* and it ensures that every infinite path π of a run gets trapped in the component Q_i of some stratum. R2 is the *eventually syntactical requirement* and it ensures that Q_i belongs to a Büchi or coBüchi stratum and that π is eventually strictly-forward.

Now we define when a run is accepting. Let π be an infinite path of a run, $\langle \rho_i, Q_i, F_i \rangle$ be the Büchi or coBüchi stratum in which π gets trapped, and $Inf(\pi)$ be the states from Q that occur infinitely many times in π . The path π is *accepting* whenever $Inf(\pi) \cap F_i \neq \emptyset$ if $\rho_i = \mathbf{B}$ and $Inf(\pi) \cap F_i = \emptyset$ otherwise (i.e. π satisfies the corresponding Büchi or coBüchi requirement). A run is *accepting* if: (i) all its infinite paths are accepting and (ii) for each vertex $(-1, q)$ reachable from the initial vertex, it holds that $q \in F_-$ (recall that F_- is the backward acceptance condition of \mathcal{A}). The ω -pointed language $\mathcal{L}_p(\mathcal{A})$ of \mathcal{A} is the set of pointed words (w, i) over Σ such that there is an accepting (i, q_0) -run of \mathcal{A} on w .

The *dual automaton* $\tilde{\mathcal{A}}$ of a two-way HAA $\mathcal{A} = \langle Q, q_0, \delta, F_-, F \rangle$ is defined as $\tilde{\mathcal{A}} = \langle q, q_0, \tilde{\delta}, Q \setminus F_-, \tilde{F} \rangle$, where $\tilde{\delta}(q, \sigma)$ is the dual formula of $\delta(q, \sigma)$ (obtained from $\delta(q, \sigma)$ by switching \vee and \wedge , and switching **true** and **false**), and \tilde{F} is obtained from F by converting a Büchi stratum $\langle \mathbf{B}, Q_i, F_i \rangle$ into the coBüchi stratum $\langle \mathbf{C}, Q_i, F_i \rangle$ and a coBüchi stratum $\langle \mathbf{C}, Q_i, F_i \rangle$ into the Büchi stratum $\langle \mathbf{B}, Q_i, F_i \rangle$. By construction the dual automaton $\tilde{\mathcal{A}}$ of \mathcal{A} is still a two-way HAA. Following standard arguments (see e.g. [4]), the dual automaton $\tilde{\mathcal{A}}$ of a two-way HAA \mathcal{A} is a two-way HAA accepting the complement of $\mathcal{L}_p(\mathcal{A})$.

B.2 Proof of Theorem 18

In this section we give the details of the translation from two-way HAA into Büchi SNWA as captured by Theorem 18 (see Appendix B.1 for a formal definition of Büchi SNWA and two-way HAA). The proposed construction is based on a preliminary result. By using the notion of odd ranking function for standard coBüchi alternating automata [1]⁶ (which intuitively, allows to convert a coBüchi acceptance condition into a Büchi-like acceptance condition) and a non-trivial generalization of the Miyano-Hayashi construction [2], we give a characterization of the pointed words in $\mathcal{L}_p(\mathcal{A})$ in terms of infinite sequences of finite sets (called *regions*) satisfying determined requirements which can be easily checked by Büchi SNWA.

Fix a two-way HAA $\mathcal{A} = \langle Q, q_0, \delta, F_-, F \rangle$ over an alphabet Σ . First, as anticipated above, we give a characterization of the fulfillment of the acceptance condition for a coBüchi stratum along a run in terms of the existence of an *odd ranking function*.

► **Definition 34.** Let $\mathcal{S} = \langle \mathbf{C}, P, F \rangle$ be a coBüchi stratum of \mathcal{A} and $n = |P|$ (the size of the stratum). For an infinite word w on Σ and a run $G = \langle V, E, v_0 \rangle$ of \mathcal{A} over w , a *ranking function of the stratum \mathcal{S} for the run G* is a function $f_{\mathcal{S}} : V \rightarrow \{1, \dots, 2n\}$ satisfying the following:

1. for all $(j, q) \in V$ such that $q \in F$, $f_{\mathcal{S}}(j, q)$ is even;

⁶ See references for the Appendix.

2. for all $(j, q), (j', q') \in V$ such that (j', q') is a successor of (j, q) in G and $q, q' \in P$, it holds that $f_S(j', q') \leq f_S(j, q)$.

Thus, since the image of f_S is bounded, for every infinite path $\pi = v_0, v_1, \dots$ of G that get trapped in the coBüchi stratum \mathcal{S} , f_S converges to a value: there is a number l such that $f_S(v_{l'}) = f_S(v_l)$ for all $l' \geq l$. We say that f_S is *odd* if for all such infinite paths π of G , f_S converges to an odd value (or, equivalently, any of such paths π visits infinitely many times vertices v such that $f_S(v)$ is odd). Note that if f_S is odd, then π is accepting. The following lemma whose proof is a straightforward generalization of the results in [1] (regarding coBüchi alternating finite-state automata), asserts that the existence of an odd ranking function is also a necessary condition for a run to be accepting.

► **Lemma 35.** *Let G be a run of \mathcal{A} over an infinite word w . G is accepting iff*

1. *for every co-Büchi stratum $\mathcal{S} = \langle C, P, F \rangle$, there is an odd ranking function of \mathcal{S} for the run G ;*
2. *every infinite path of G which get trapped in the component of a Büchi stratum $\mathcal{S} = \langle B, P, F \rangle$ satisfies the Büchi acceptance condition F ;*
3. *for each vertex $(-1, q)$ reachable from the initial vertex, $q \in F_-$ (recall that F_- is the backward acceptance condition of \mathcal{A}).*

Now, based on Lemma 35 and the classical breakpoint construction [2],⁷ we give a characterization of the pointed words $(w, \ell) \in \mathcal{L}_p(\mathcal{A})$ in terms of infinite sequences of finite sets (called *regions*) satisfying determined requirements which can be easily checked by Büchi SNWA. A coBüchi state is a state of \mathcal{A} belonging to some coBüchi stratum of \mathcal{A} . For a coBüchi state q , a *rank* of q is a natural number in $\{1, \dots, 2n\}$, where n is the size of the stratum of q . A *region* of \mathcal{A} is a triple (R, O, f) , where $R \subseteq Q$ is a set of states, $O \subseteq R$, and f is a mapping assigning to each coBüchi state $q \in R$ a rank of q such that $f(q)$ is even if $q \in F$, where $\langle C, P, F \rangle$ is the coBüchi stratum of q . A state q of \mathcal{A} is *accepting* with respect to f if (1) either q is an accepting state of a Büchi stratum, or (2) q is a coBüchi state and, additionally, $f(q)$ is odd if $q \in R$. The *stop region* is the region (F_-, \emptyset, f) where $f : Q \mapsto \{1\}$ and F_- is the backward acceptance condition of \mathcal{A} .

For an atom (dir, q) of \mathcal{A} and a position $i \geq 0$, the *effect* of (the move) (dir, q) w.r.t. i is the pair (j, q) , where $j = i + 1$ if $dir = \rightarrow$, and $j = i - 1$ otherwise. Let (w, ℓ) be a pointed word over Σ and $\nu = (R_0, O_0, f_0), (R_1, O_1, f_1), \dots$ be an infinite sequence of regions. We say that ν is *good with respect to* (w, ℓ) if for all $i \geq 0$, there is a mapping g_i assigning to each $q \in R_i$ a minimal model of $\delta(q, w(i))$ such that the following holds, where Acc_i denotes the set of accepting states of \mathcal{A} with respect to f_i , and $(R_{-1}, \emptyset, f_{-1})$ is the stop region:

- *Initialization.* $q_0 \in R_\ell$.
- *δ -consistency w.r.t. g_i .* For all $q \in R_i$ and $(dir, p) \in g_i(q)$, let (h, p) be the effect of (dir, p) w.r.t. i ; then, $p \in R_h$. Additionally, if q and p are coBüchi states belonging to the same stratum, then $f_h(p) \leq f_i(q)$ (*ranking requirement w.r.t. g_i*).
- *Miyano-Hayashi requirement w.r.t. g_i .* For all $q \in O_i$ and $(\rightarrow, p) \in g_i(q)$ such that $p \in R_{i+1} \setminus Acc_{i+1}$, it holds that $p \in O_{i+1}$.

The infinite sequence of regions ν is *accepting* iff there are infinitely many positions $i \geq 0$ such that $O_i = \emptyset$ and $O_{i+1} = R_{i+1} \setminus Acc_{i+1}$ (*acceptance requirement*).

⁷ See references for the Appendix.

Intuitively, the infinite sequence of regions ν represents a graph $G = \langle V \subseteq (\mathbb{N} \cup \{-1\}) \times Q, E, v_0 \rangle$ where for all input positions $i \geq 0$, R_i is the set of vertices of G associated with position i . The initialization and δ -consistency requirement ensure that G is a (ℓ, q_0) -run of \mathcal{A} over w and for each vertex $(-1, q)$ reachable from the initial vertex, $q \in F_-$. Additionally, the ranking requirement ensures that for each non-trivial coBüchi stratum \mathcal{S} , there is a ranking function $f_{\mathcal{S}}$ of \mathcal{S} for the run G . By Lemma 35, the run is accepting if $f_{\mathcal{S}}$ is odd and Condition 2 in Lemma 35 holds. This, in turn, is equivalent to require that every infinite path of G visits infinitely many vertices in Acc , where Acc is the set of G -vertices (i, q) such that $q \in Acc_i$. This condition is captured by the Miyano-Hayashi and the acceptance requirements on the sets O_i . Formally, the following holds.

► **Lemma 36** (Characterization lemma for HAA). *$(w, \ell) \in \mathcal{L}_p(\mathcal{A})$ iff there is an accepting infinite sequence of regions which is good with respect to (w, ℓ) .*

Proof. \Leftarrow) First, we prove the if direction. Assume that there is an accepting infinite sequence of regions $\nu = (R_0, O_0, f_0), (R_1, O_1, f_1), \dots$ which is good with respect to the pointed word (w, ℓ) . We need to show that $(w, \ell) \in \mathcal{L}_p(\mathcal{A})$. For all $i \geq 0$, let Acc_i be the set of accepting states of \mathcal{A} with respect to f_i , and g_i be the mapping assigning to each $q \in R_i$ a minimal model of $\delta(q, w(i))$ such that ν satisfies the δ -consistency requirement, the ranking requirement, and the Miyano-Hayashi requirement w.r.t. g_i . Let P_s be the set of states $p \in Q$ such that for some $q \in R_0$, $(\leftarrow, p) \in g_0(q)$. Note that the δ -consistency requirement ensures that P_s contains only states belonging to the backward acceptance condition F_- of \mathcal{A} . We define a graph $G = \langle V, E, v_0 \rangle$ and show that it is an accepting (ℓ, q_0) -run of \mathcal{A} over w . The graph G is defined as follows:

- $v_0 = (\ell, q_0)$, $V \subseteq (\mathbb{N} \cup \{-1\}) \times Q$ such that: (i) $(-1, q) \in V$ iff $q \in P_s$ and (ii) for all $i \geq 0$, $(i, q) \in V$ iff $q \in R_i$;
- there is an edge from (i, q) to (j, p) iff $i \geq 0$ and for some $(dir, p) \in g_i(q)$, (j, p) is the effect of (dir, p) w.r.t. i .

Since the sequence of regions ν satisfies the initialization requirement and the δ -consistency requirement w.r.t. g_i for all $i \geq 0$, G is a (ℓ, q_0) -run of \mathcal{A} over w . It remains to show that G is accepting. We assume the contrary and derive a contradiction. Then, since \mathcal{A} is a two-way HAA and the acceptance condition for the vertices $(-1, q)$ is satisfied, there must be a strictly-forward infinite path $\pi = (i, q_i), (i+1, q_{i+1}), \dots$ of G for some $i \geq 0$ such that the following holds:

- for some Büchi stratum $\langle B, P, F \rangle$, $q_h \in P \setminus F$, for all $h \geq i$. Since $q_h \in R_h$, we obtain that $q_h \in R_h \setminus Acc_h$ for all $h \geq i$.
- for some coBüchi stratum $\langle C, P, F \rangle$, $q_h \in P$ for all $h \geq i$, and for infinitely many $k \geq i$, $q_k \in F$. Since ν satisfies the ranking requirement w.r.t. g_h , $f_{h+1}(q_{h+1}) \leq f_h(q_h)$ for all $h \geq i$. It follows that there is $k \geq i$ such that $q_k \in F$ and for all $h \geq k$, $f_h(q_h) = f_k(q_k)$. In particular, $f_h(q_h)$ is even. Hence, for all $h \geq k$, $q_h \in R_h \setminus Acc_h$.

Thus, we obtain that there is an infinite strictly forward path $\pi = (k, q_k), (k+1, q_{k+1}), \dots$ of G such that $q_h \in R_h \setminus Acc_h$ for all $h \geq k$. Since the sequence of regions ν is accepting, there must be $i \geq k$ such that $O_i = R_i \setminus Acc_i \neq \emptyset$. Moreover, since ν satisfies the Miyano-Hayashi requirement w.r.t. the mappings g_j , we deduce that $O_j \neq \emptyset$ for all $j > i$, which contradicts the assumption that the sequence of regions ν is accepting.

\Rightarrow) Now, we prove the only if direction. Let $(w, \ell) \in \mathcal{L}_p(\mathcal{A})$. Hence, there is an accepting (ℓ, q_0) -run $G = \langle V, E, v_0 \rangle$ of \mathcal{A} over w . By Lemma 35, for every coBüchi stratum \mathcal{S} of \mathcal{A} ,

there is an odd ranking function f_S of S for the run G . Let Acc be the set of vertices (i, q) of the run G such that (1) either q is an accepting state of a Büchi stratum, or (2) q belongs to a coBüchi stratum S and $f_S(i, q)$ is odd. Since G is accepting and every infinite path of G gets eventually trapped either in a Büchi stratum or a coBüchi stratum, it holds that every infinite path of G visits infinitely many times vertices in Acc . We define an infinite sequence of regions $\nu = (R_0, O_0, f_0), (R_1, O_1, f_1), \dots$ and show that it is accepting and good with respect to the pointed word (w, ℓ) , hence, the result follows. For all $i \geq 0$, R_i and f_i are defined as follows:

- $R_i := \{(i, q) \mid (i, q) \in V\};$
- for all coBüchi strata $S = \langle C, P, F \rangle$ and $q \in R_i \cap P$, $f_i(q) = f_S(i, q)$.

Note that since $q_0 \in R_\ell$, the sequence ν (independently of the form of the sets O_i) satisfies the initialization requirement (w.r.t. (w, ℓ)). Let Acc_i be the set of the accepting states of \mathcal{A} with respect to f_i . Note that for all $q \in R_i$, $q \in Acc_i$ iff $(i, q) \in Acc$. Since G is a run over w , for all $i \geq 1$, there must be a mapping g_i over R_i such that for all $q \in R_i$, $g_i(q)$ is a minimal model of $\delta(q, w(i))$ and the sequence ν (independently of the form of the sets O_i) satisfies the δ -consistency requirement w.r.t. g_i . Moreover, since for every coBüchi stratum S of \mathcal{A} , f_S is an odd ranking function of S for the run G , the sequence ν (independently of the form of the sets O_i) satisfies the ranking requirement w.r.t. g_i . It remains to define the sets O_i and show that the resulting sequence is accepting and satisfies the Miyano-Hayashi requirement as well. For this, we use the following claim.

Claim: there is an infinite sequence $0 = h_1 < h_2 < \dots$ of positions of w such that for all $j \geq 0$ and finite paths of G of the form $\pi = (h_j, p), \dots, (h_{j+1} - 1, q)$, π visits some state in Acc .

First, we show that the result follows from the claim above and then we prove the claim. So, let $0 = h_1 < h_2 < \dots$ be an infinite sequence of positions of w satisfying the claim above. For every $i \geq 0$, let $j \geq 0$ be the unique natural number such that $h_j \leq i < h_{j+1}$. Then, O_i is defined as follows:

- O_i is the set of states q such that there is a finite path of G of the form $\pi = (h_j, p), \dots, (i, q)$ which does *not* visit vertices in Acc .

Note that $O_i \cap Acc_i = \emptyset$ and $O_i \subseteq R_i$. By construction and the claim above, we have that for all $j > 0$, $O_{h_j-1} = \emptyset$ and $O_{h_j} = R_{h_j} \setminus Acc_{h_j}$. Hence, the infinite sequence of regions $\nu = (R_0, O_0, f_0), (R_1, O_1, f_1), \dots$ is accepting. For the Miyano-Hayashi requirement w.r.t. g_i , let $q \in O_i$ and $(\rightarrow, p) \in g_i(q)$ such that $p \notin Acc_{i+1}$ (hence, $(i+1, p) \notin Acc$). We need to show that $p \in O_{i+1}$. Let $j \geq 0$ such that $h_j \leq i < h_{j+1}$. Since $O_i \neq \emptyset$ and $O_{h_{j+1}-1} = \emptyset$, we have that $i < h_{j+1} - 1$. Hence, $i+1 < h_{j+1}$. Thus, since $q \in O_i$ and $(i+1, p)$ is a successor of (i, q) in G which is not in Acc , we obtain that $p \in O_{i+1}$. Therefore, $\nu = (R_0, O_0, f_0), (R_1, O_1, f_1), \dots$ is an accepting infinite sequence of regions which is good w.r.t. the pointed word (w, ℓ) . It remains to prove the claim.

Proof of the claim: fix $k \geq 0$. For each $i \geq 0$, let T_i be the set of states $q \in Q$ such that there is a finite path of G of the form $(k, p), \dots, (i, q)$ which does *not* visit Acc -vertices. Since k is arbitrary, in order to prove the claim, it suffices to show that there is a position $m > k$ such that $T_{m-1} = \emptyset$. Let $H = \{(i, q) \in \mathbb{N} \times Q \mid q \in T_i\}$. Note that $H \cap Acc = \emptyset$. First, we prove that the set H is finite. We assume the contrary and derive a contradiction. Let G_H be the subgraph of G given by the restriction of G to the set of vertices H . Note that by construction, every vertex in G_H is reachable in G_H from a vertex of the form (k, p) .

Moreover, each vertex of G_H has only finitely many successors. Since G_H is infinite and the set of vertices of the form (k, p) is finite, by König's Lemma, G_H contains an infinite path π . This is a contradiction since π does not visit vertices in Acc and π is also an infinite path of G . Thus, the set $H = \{(i, q) \in \mathbb{N} \times Q \mid q \in T_i\}$ is finite. It follows that there is $j \geq 0$ such that for all $i \geq j$, $T_j = \emptyset$. Hence, the result follows, which concludes the proof of the claim and the lemma as well. \blacktriangleleft

Now, we can prove Theorem 18.

► **Theorem 18.** *For a two-way HAA \mathcal{A} with n states, one can construct “on the fly” and in singly exponential time a Büchi SNWA accepting $\mathcal{L}_p(\mathcal{A})$ with $2^{O(n \cdot \log(n))}$ states.*

Proof. For the fixed two-way HAA $\mathcal{A} = \langle Q, q_0, \delta, F_-, F_+ \rangle$ over Σ , we construct a Büchi SNWA $\mathcal{A}_N = \langle P, P_0, \rho, F'_-, F'_+ \rangle$ over Σ accepting $\mathcal{L}_p(\mathcal{A})$ with $2^{O(|Q| \cdot \log(|Q|))}$ states. We construct the Büchi SNWA \mathcal{A}_N in such a way that given a pointed word (w, i) over Σ , \mathcal{A}_N accepts (w, i) iff there is an *accepting* infinite sequence of regions of \mathcal{A} which is good w.r.t. (w, i) . At each step, the forward (resp., backward) copy of the automaton keeps tracks in its control state of the guessed region associated with the current input position and the guessed region associated with the previous (resp., next) input position. Note that in this way, the automaton can check locally (i.e., by its transition function) that the guessed infinite sequence of regions satisfies the δ -consistency requirement, the ranking requirement, and the Miyano-Hayashi requirement. Finally, the Büchi acceptance condition of \mathcal{A}_N is used to check that the guessed sequence of regions is accepting.

In order to simplify the formal definition of \mathcal{A}_N , we introduce additional notation. For a region $\mathcal{R} = (R, O, f)$ and $\sigma \in \Sigma$, a (\mathcal{R}, σ) -model is a mapping assigning to each $q \in R$, a minimal model of $\delta(q, \sigma)$. For a direction $dir \in \{\rightarrow, \leftarrow\}$, two regions $\mathcal{R} = (R, O, f)$ and $\mathcal{R}_{dir} = (R_{dir}, O_{dir}, f_{dir})$, and a (\mathcal{R}, σ) -model g for some $\sigma \in \Sigma$, we say that \mathcal{R} is *dir-consistent w.r.t. g* and \mathcal{R}_{dir} if the following holds:

- *δ -consistency requirement.* For all $q \in R$ and $(dir, p) \in g(q)$, $p \in R_{dir}$. If, additionally, p and q are coBüchi states belonging to the same stratum, then $f_{dir}(p) \leq f(q)$ (*Ranking requirement*).
- *Miyano-Hayashi requirement.* If $dir = \rightarrow$, then for all $q \in O$ and $(dir, p) \in g(q)$, whenever p is not accepting w.r.t. f_{dir} , then $p \in O_{dir}$.

Formally, the Büchi SNWA $\mathcal{A}_N = \langle P, P_0, \rho, F'_-, F'_+ \rangle$ is defined as follows:

- $P = (REG \times REG) \cup (in \times REG \times REG) \cup \{stop\}$, where REG is the set of regions.
- P_0 is the set of states of the form $(in, \mathcal{R}, (R, O, f))$ such that $q_0 \in R$.
- the transition function ρ is defined as follows, where \mathcal{R}_s is the stop region:
 - *Forward transitions:* $p' \in \rho(p, \sigma, \rightarrow)$ iff (either $p = (\mathcal{R}_-, \mathcal{R})$ or $p = (in, \mathcal{R}_-, \mathcal{R})$), $p' = (\mathcal{R}, \mathcal{R}_+)$ and there is a (\mathcal{R}, σ) -model g such that \mathcal{R} is \rightarrow -consistent w.r.t. g and \mathcal{R}_+ and \leftarrow -consistent w.r.t. g and \mathcal{R}_- .
 - *Backward transitions:* $p' \in \rho(p, \sigma, \leftarrow)$ iff one of the following holds:
 - * $p' = stop$, and either $p = (in, \mathcal{R}_s, \mathcal{R})$ or $p = (\mathcal{R}_s, \mathcal{R})$;
 - * $p = (in, \mathcal{R}, \mathcal{R}_+)$ and $p' = (\mathcal{R}, \mathcal{R}_+)$;
 - * $p = (\mathcal{R}, \mathcal{R}_+)$, $p' = (\mathcal{R}_-, \mathcal{R})$ and there is a (\mathcal{R}, σ) -model g such that \mathcal{R} is \rightarrow -consistent w.r.t. g and \mathcal{R}_+ and \leftarrow -consistent w.r.t. g and \mathcal{R}_- .
- $F'_- = \{stop\}$.
- F'_+ consists of the states of the form $((\mathcal{R}_-, \emptyset, f_-), (R, O, f))$ such that $O = R \setminus Acc$, where Acc is the set of accepting states of \mathcal{A} w.r.t. f .

By construction, it easily follows that $(w, i) \in \mathcal{L}_p(\mathcal{A}_N)$ iff there is an accepting infinite sequence of regions which is good w.r.t. (w, i) . By Lemma 36, it follows that $\mathcal{L}_p(\mathcal{A}_N) = \mathcal{L}_p(\mathcal{A})$. Since the number of regions is at most $2^{2|Q|} \cdot 2^{|Q| \cdot \log(2|Q|)}$, Theorem 18 follows. ◀

B.3 Proof of Theorem 19

In this Subsection we provide a proof Theorem 19 (see Appendix B.1 for a formal definition of Büchi SNWA and two-way HAA). We will use the following trivial result.

► **Proposition 37.** *A Büchi SNWA \mathcal{A} can be converted “on the fly” in linear time into a two-way HAA accepting $\mathcal{L}_p(\mathcal{A})$.*

► **Theorem 19.** *Let φ be a first-level existential (resp., first-level universal) QPTL formula and $h = \text{sad}(\varphi)$. Then, one can construct “on the fly” a Büchi SNWA \mathcal{A}_φ accepting $\mathcal{L}_p(\varphi)$ in time $\text{Tower}(h, O(|\varphi|))$ (resp., $\text{Tower}(h + 1, O(|\varphi|))$).*

Proof. The proof is by induction on $|\varphi|$. The base case $|\varphi| = 1$ is trivial. Now, assume that $|\varphi| > 1$. We distinguish four cases depending on the type of root operator of φ (either temporal modality, or existential quantifier, or universal quantifier, or boolean connective).

Case 1: the root operator of φ is a temporal modality. Let $h = \text{sad}(\varphi)$ and

$$P := \{\exists p_1. \theta_1, \dots, \exists p_n. \theta_n, \forall q_1. \xi_1, \dots, \forall q_k. \xi_k\}$$

be the set of quantified subformulas of φ which do not occur in the scope of a quantifier. If $P = \emptyset$, then φ is a PLTL formula. In this case, by a straightforward adaptation of the standard translation of LTL into Büchi word automata [3],⁸ one can construct a Büchi SNWA of size $2^{O(|\varphi|)}$ accepting $\mathcal{L}_p(\varphi)$. Hence, the result follows.

Assume now that $P \neq \emptyset$. Then, φ can be viewed as a PLTL formula in positive normal form, written $\text{PLTL}(\varphi)$, over the set of atomic proposition given by P .

We first, assume that for each $\psi \in P$, $\text{sad}(\psi) < \text{sad}(\varphi)$. Hence, for all $\psi \in P$, $\text{sad}(\psi) \leq h - 1$ and $h > 1$. Moreover, in this case, φ must be a first-level existential formula. For all $1 \leq j \leq k$, let $\tilde{\xi}_j$ be the positive normal form of $\neg \xi_j$. Note that $\text{sad}(\forall q_i. \xi_i) = \text{sad}(\neg \exists q_i. \tilde{\xi}_i)$ and $\mathcal{L}_p(\forall q_i. \xi_i) = \mathcal{L}_p(\neg \exists q_i. \tilde{\xi}_i)$. Thus, by applying the induction hypothesis, Proposition 37 and the complementation lemma for two-way HAA, it follows that for each $\psi \in P$, one can construct “on the fly” in time at most $\text{Tower}(h - 1, O(|\varphi|))$, a two-way HAA \mathcal{A}_ψ accepting $\mathcal{L}_p(\psi)$. Then, by an easy generalization of the standard linear-time translation of LTL formulas into Büchi alternating word automata and by using the two-way HAA \mathcal{A}_ψ with $\psi \in P$, one can construct “on the fly”, in time $\text{Tower}(h - 1, O(|\varphi|))$, a two-way HAA \mathcal{A}_φ accepting $\mathcal{L}_p(\varphi)$. Intuitively, given an input pointed word, each copy of \mathcal{A}_φ keeps track of the current subformula of $\text{PLTL}(\varphi)$ which needs to be evaluated. The evaluation simulates the semantics of PLTL (in positive normal form) by using universal and existential branching, but when the current subformula ψ is in P , then the current copy of \mathcal{A}_φ activates a copy of \mathcal{A}_ψ in the initial state.

Formally, for each $\psi \in P$, let $\mathcal{A}_\psi = \langle Q_\psi, q_\psi, \delta_\psi, F_\psi^-, F_\psi \rangle$. Without loss of generality, we assume that the state sets of the two-way \mathcal{A}_ψ are pairwise distinct. Then, $\mathcal{A}_\varphi = \langle Q, q_0, \delta, F^-, F \rangle$, where

⁸ See references for the Appendix.

- $Q = \bigcup_{\psi \in P} Q_\psi \cup \text{Sub}(\varphi)$, where $\text{Sub}(\varphi)$ is the set of subformulas of $\text{PLTL}(\varphi)$;
- $q_0 = \varphi$;
- The transition function δ is defined as follows: $\delta(q, \sigma) = \delta_\psi(q, \sigma)$ if $q \in Q_\psi$ for some $\psi \in P$. If instead $q \in \text{Sub}(\varphi)$, then $\delta(q, \sigma)$ is defined by induction on the structure of q as follows:
 - $\delta(p, \sigma) = \text{true}$ if $p \in \sigma$, and $\delta(p, \sigma) = \text{false}$ otherwise (for all $p \in \text{AP} \cap \text{Sub}(\varphi)$);
 - $\delta(\neg p, \sigma) = \text{false}$ if $p \in \sigma$, and $\delta(\neg p, \sigma) = \text{true}$ otherwise (for all $p \in \text{AP} \cap \text{Sub}(\varphi)$);
 - $\delta(\phi_1 \wedge \phi_2, \sigma) = \delta(\phi_1, \sigma) \wedge \delta(\phi_2, \sigma)$ and $\delta(\phi_1 \vee \phi_2, \sigma) = \delta(\phi_1, \sigma) \vee \delta(\phi_2, \sigma)$;
 - $\delta(\mathbf{X}\phi, \sigma) = (\rightarrow, \phi)$ and $\delta(\mathbf{X}^-\phi, \sigma) = (\leftarrow, \phi)$;
 - $\delta(\phi_1 \mathbf{U} \phi_2, \sigma) = \delta(\phi_2, \sigma) \vee (\delta(\phi_1, \sigma) \wedge (\rightarrow, \phi_1 \mathbf{U} \phi_2))$;
 - $\delta(\phi_1 \mathbf{U}^-\phi_2, \sigma) = \delta(\phi_2, \sigma) \vee (\delta(\phi_1, \sigma) \wedge (\leftarrow, \phi_1 \mathbf{U}^-\phi_2))$;
 - $\delta(\phi_1 \mathbf{R} \phi_2, \sigma) = \delta(\phi_2, \sigma) \wedge (\delta(\phi_1, \sigma) \vee (\rightarrow, \phi_1 \mathbf{R} \phi_2))$;
 - $\delta(\phi_1 \mathbf{R}^-\phi_2, \sigma) = \delta(\phi_2, \sigma) \wedge (\delta(\phi_1, \sigma) \vee (\leftarrow, \phi_1 \mathbf{R}^-\phi_2))$;
 - for each $\psi \in P$, $\delta(\psi, \sigma) = \delta(q_\psi, \sigma)$.
- $F_- = \bigcup_{\psi \in P} F_\psi^-$
- $F = \bigcup_{\psi \in P} F_\psi \vee \bigcup_{\phi \in \text{Sub}(\varphi)} \mathcal{S}_\phi$, where for each $\phi \in \text{Sub}(\varphi)$, \mathcal{S}_ϕ is defined as follows:
 - if ϕ has as root a past temporal modality, then \mathcal{S}_ϕ is the negative stratum $(\{\phi\}, -, \emptyset)$;
 - if ϕ has as root the (future) until modality, then \mathcal{S}_ϕ is the Büchi stratum $(\{\phi\}, \mathbf{B}, \emptyset)$;
 - if ϕ has as root the (future) release modality, then \mathcal{S}_ϕ is the coBüchi stratum $(\{\phi\}, \mathbf{C}, \emptyset)$;
 - otherwise, \mathcal{S}_ϕ is the transient stratum given by $(\{\phi\}, \mathbf{t}, \emptyset)$.

Finally, since $h > 1$ and the size of the two-way HAA \mathcal{A}_φ is $\text{Tower}(h-1, O(|\varphi|))$, by applying Theorem 18, one can construct “on the fly” a Büchi SNWA accepting $\mathcal{L}_p(\varphi)$ of size $\text{Tower}(h, O(|\varphi|))$. Hence, the result follows.

Now, assume that for some $\psi \in P$, $\text{sad}(\psi) = \text{sad}(\varphi)$. Let $h = \text{sad}(\varphi)$. There are two cases:

- $\psi = \exists p. \psi'$. Since the root of φ is a temporal modality, by definition of strong alternation depth, either $\varphi = F^-\varphi'$ or $\varphi = F\varphi'$ (and ψ is a subformula of φ'). Moreover, φ and φ' must be first-level existential formulas. Hence, by applying the induction hypothesis, the result directly follows from the following claim.

Claim. Given a Büchi SNWA \mathcal{A} , one can construct “on the fly” and in linear time two Büchi SNWA \mathcal{A}_+ and \mathcal{A}_- such that

- $\mathcal{L}_p(\mathcal{A}_+) = \{(w, i) \mid \text{for some } j \geq i \ (w, j) \in \mathcal{L}_p(\mathcal{A})\}$;
- $\mathcal{L}_p(\mathcal{A}_-) = \{(w, i) \mid \text{for some } j \leq i \ (w, j) \in \mathcal{L}_p(\mathcal{A})\}$.

Proof of the Claim. We illustrate the construction of \mathcal{A}_+ (the construction of \mathcal{A}_- being similar). Intuitively, given an input pointed word (w, i) , \mathcal{A}_+ guesses a position $j \geq i$ and checks that $(w, j) \in \mathcal{L}_p(\mathcal{A})$ as follows. Initially, \mathcal{A}_+ keeps track of a guessed state q of \mathcal{A} which represents the state where the backward copy of \mathcal{A} would be on reading the i^{th} position of w in some guessed accepting run of \mathcal{A} over (w, j) . If $j = i$, then q needs to be some initial state of \mathcal{A} , and \mathcal{A}_+ simply simulates the behavior of \mathcal{A} on (w, i) . Otherwise, \mathcal{A}_+ splits in two copies: the backward copy simulates the backward copy of \mathcal{A} , while the forward copy of \mathcal{A}_+ behaves as follows. In the first step, the forward copy of \mathcal{A} moves to the same state q , and after this step, such a copy starts to simulate in forward-mode the backward copy of \mathcal{A} until, possibly, a ‘switch’ occurs at the guessed position j , where the forward copy of \mathcal{A}_+ simulates in a unique step from the current state some initial

split of \mathcal{A} in the backward and forward copy. After such a switch (if any), the forward copy of \mathcal{A}_+ simply simulates the forward copy of \mathcal{A} . We use two flags to distinguish the different phases of the simulation (in particular, the initial phase and the switch phase). Formally, let $\mathcal{A} = \langle Q, Q_0, \rho, F_-, F_+ \rangle$. Then, $\mathcal{A}_+ = \langle Q', Q'_0, \rho', F'_-, F'_+ \rangle$, where $Q' = Q \times \{\perp, \top\} \times \{\text{init}, \text{no-init}\}$, $Q'_0 = Q \times \{\perp\} \times \{\text{init}\}$, $F'_- = F_- \times \{\top\} \times \{\text{no-init}\}$, $F'_+ = F_+ \times \{\top\} \times \{\text{no-init}\}$, and ρ' is defined as follows:

- Backward moves: $(q', f'_1, f'_2) \in \rho'((q, f_1, f_2), \leftarrow, \sigma)$ iff $f'_1 = \top$, $f'_2 = \text{no-init}$, and $q' \in \rho(q, \leftarrow, \sigma)$;
- Forward moves: $(q', f'_1, f'_2) \in \rho'((q, f_1, f_2), \rightarrow, \sigma)$ iff one of the following holds:
 - * $f_2 = \text{init}$, $f'_2 = \text{no-init}$, and either $q' = q$ and $f'_1 = \perp$, or $q \in Q_0$, $q' \in \rho(q, \rightarrow, \sigma)$, and $f'_1 = \top$ (*initialization*);
 - * $f'_2 = f_2 = \text{no-init}$, $f'_1 = \perp$, and $q \in \rho(q', \leftarrow, \sigma)$ (*simulation of backward moves*);
 - * $f'_2 = f_2 = \text{no-init}$, $f_1 = \perp$, $f'_1 = \top$, and there is $q_0 \in Q$ such that $q \in \rho(q_0, \leftarrow, \sigma)$ and $q' \in \rho(q_0, \rightarrow, \sigma)$ (*switch*);
 - * $f'_2 = f_2 = \text{no-init}$, $f'_1 = f_1 = \top$, and $q' \in \rho(q, \rightarrow, \sigma)$ (*simulation of the forward moves of \mathcal{A} after the switch*).
- $\psi = \forall p. \psi'$. Since the root of φ is a temporal modality and $\text{sad}(\psi) = \text{sad}(\varphi) = h$, by definition of strong alternation depth, either $\varphi = G^-\varphi'$ or $\varphi = G\varphi'$ (and ψ is a subformula of φ'). Moreover, φ and φ' must be first-level universal formulas and $\text{sad}(\varphi') = h$. Assume that $\varphi = G\varphi'$ (the other case being similar). Let $\tilde{\varphi}'$ be the positive normal form of $\neg\varphi'$. Note that $\text{sad}(\neg F\tilde{\varphi}') = h$ and $\mathcal{L}_p(F\tilde{\varphi}') = \mathcal{L}_p(\neg\varphi)$. Hence, by the previous case, one can construct “on the fly” a Büchi SNWA $\mathcal{A}_{\neg\varphi}$ of size $\text{Tower}(h, O(|\varphi|))$ accepting $\mathcal{L}_p(\neg\varphi)$. By Proposition 37, the complementation lemma for two-way HAA and Theorem 18, it follows that one can construct “on the fly” a Büchi SNWA \mathcal{A}_φ of size $\text{Tower}(h+1, O(|\varphi|))$ accepting $\mathcal{L}_p(\varphi)$. Hence, the result follows.

Case 2: φ is an existential quantified formula of the form $\varphi = \exists p. \varphi'$. Hence, in particular, φ is a first-level existential formula. Let $h = \text{sad}(\varphi)$ and $h' = \text{sad}(\varphi')$. We observe that like Büchi nondeterministic automata, SNWA are efficiently closed under projection. In particular, given a Büchi SNWA \mathcal{A} over 2^{AP} and $p \in \text{AP}$, one can construct “on the fly” and in linear time a Büchi SNWA accepting the language $\{w \in (2^{\text{AP}})^\omega \mid \text{there is } w' \in \mathcal{L}_p(\mathcal{A}) \text{ such that } w' =_{\text{AP} \setminus \{p\}} w\}$. Thus, by applying the induction hypothesis, it follows that one can construct “on the fly” a Büchi SNWA accepting $\mathcal{L}_p(\varphi)$ of size $\text{Tower}(h', O(|\varphi'|))$ if φ' is a first-level existential formula, and of size $\text{Tower}(h' + 1, O(|\varphi'|))$ otherwise. Since $h' \leq h$, and $h' = h - 1$ if φ' is a first-level universal formula, the result follows.

Case 3: φ is an universal quantified formula of the form $\varphi = \forall p. \varphi'$. Hence, in particular, φ is a first-level universal formula. Let $h = \text{sad}(\varphi)$ and $\tilde{\varphi}'$ be the positive normal form of $\neg\varphi'$. Note that $\text{sad}(\neg \exists p. \tilde{\varphi}') = h$ and $\mathcal{L}_p(\exists p. \tilde{\varphi}') = \mathcal{L}_p(\neg\varphi)$. Hence, by Case 2, one can construct “on the fly” a Büchi SNWA $\mathcal{A}_{\neg\varphi}$ of size $\text{Tower}(h, O(|\varphi|))$ accepting $\mathcal{L}_p(\neg\varphi)$. By Proposition 37, the complementation lemma for two-way HAA and Theorem 18, it follows that one can construct “on the fly” a Büchi SNWA \mathcal{A}_φ of size $\text{Tower}(h+1, O(|\varphi|))$ accepting $\mathcal{L}_p(\varphi)$. Hence, the result follows.

Case 4: φ is of the form $\varphi = \varphi_1 \wedge \varphi_2$ or $\varphi = \varphi_1 \vee \varphi_2$. Assume that $\varphi = \varphi_1 \wedge \varphi_2$ (the other case being similar). Let $h_1 = \text{sad}(\varphi_1)$, $h_2 = \text{sad}(\varphi_2)$, and $h = \text{sad}(\varphi)$. Note that $h = \max(h_1, h_2)$. We use the fact that like Büchi nondeterministic automata, SNWA are trivially and efficiently closed under intersection. In particular, given two Büchi SNWA \mathcal{A}_1

and \mathcal{A}_2 , one can construct “on the fly” and in time $O(|\mathcal{A}_1||\mathcal{A}_2|)$ a Büchi SNWA accepting the language $\mathcal{L}_p(\mathcal{A}_1) \cap \mathcal{L}_p(\mathcal{A}_2)$. We distinguish two cases:

- φ is a first-level existential formula: assume that $h = h_1 = h_2$ (the other cases, i.e., when either $h = h_1$ and $h_2 < h$, or $h = h_2$ and $h_1 < h$, are similar). Hence, both φ_1 and φ_2 are existential. Since $h = \max(h_1, h_2)$, by applying the induction hypothesis and the closure of SNWA under intersection, it follows that one can construct “on the fly” a Büchi SNWA accepting the language $\mathcal{L}_p(\varphi)$ whose size is at most $\text{Tower}(h_1, O(|\varphi_1|)) \cdot \text{Tower}(h_2, O(|\varphi_2|)) = \text{Tower}(h, O(|\varphi|))$. Hence, in this case, the result follows.
 - φ is a first-level universal formula: hence, there is $j = 1, 2$ such that φ_j is a first-level universal formula and $h_j = h$. Since $h = \max(h_1, h_2)$, by applying the induction hypothesis and the closure of SNWA under intersection, it follows that one can construct “on the fly” a Büchi SNWA accepting the language $\mathcal{L}_p(\varphi)$ whose size is at most $\text{Tower}(h_1 + 1, O(|\varphi_1|)) \cdot \text{Tower}(h_2 + 1, O(|\varphi_2|)) = \text{Tower}(h + 1, O(|\varphi|))$. Hence, the result follows.
- This concludes the proof of Theorem 19. ◀

B.4 Lower bounds in Theorem 16

For each $h \geq 1$, let QPTL^h be the fragment of QPTL consisting of formulas whose strong alternation depth is at most h . In this section, for all $h \geq 1$, we provide the lower bounds for QPTL^h and the existential fragment of QPTL^h as captured by Theorem 16. We focus on the existential fragment of QPTL^h . The proof of h -EXPSPACE-hardness of unrestricted QPTL^h is simpler.⁹ Therefore, in the rest of this section, we show that satisfiability for the *existential fragment* of QPTL^h is $(h - 1)$ -EXPSPACE-hard even for formulas using temporal modalities in $\{X, X^-, F, F^-, G, G^-\}$. This is proved by a reduction from the non-halting problem for $\exp[h - 1]$ -space bounded deterministic Turing Machines, where $\exp[h - 1]$ denotes the class of functions $f : \mathbb{N} \rightarrow \mathbb{N}$ such that for some constant $c \geq 1$, $f(n) = \text{Tower}(h - 1, n^c)$ for each $n \in \mathbb{N}$.

Let AP be the infinite set of atomic propositions given by

$$\text{AP} := \{0, 1\} \cup \{\$1, \$2, \dots\}$$

Moreover, for each $h \geq 1$, let AP_h be the finite subset of AP given by

$$\text{AP}_h := \{0, 1\} \cup \{\$1, \dots, \$h\}$$

First, for all $n \geq 1$ and $h \geq 1$, we define an encoding of the natural numbers in $[0, \text{Tower}(h, n) - 1]$ by finite words over AP_h , called (h, n) -codes. In particular, for $h > 1$, an (h, n) -code encoding a natural number $m \in [0, \text{Tower}(h, n) - 1]$ is a sequence of $\text{Tower}(h - 1, n)$ $(h - 1, n)$ -codes, where the i^{th} $(h - 1, n)$ -code encodes both the value and (recursively) the position of the i^{th} -bit in the binary representation of m . Formally, the set of (h, n) -codes is defined by induction on h as follows.

Base Step: $h = 1$. A $(1, n)$ -code is a finite word w over AP_1 of the form $w = \$1bb_1 \dots b_n\1 , where $b, b_1, \dots, b_n \in \{0, 1\}$. The *content* of w is the bit b and the *index* of w is the natural

⁹ Note that by the well-known h -EXPSPACE-hardness of satisfiability of QPTL formulas in prenex form whose alternation depth of existential and universal quantifiers is at most h , we immediately deduce $(h - 1)$ -EXPSPACE-hardness for satisfiability of unrestricted QPTL^h . One can enforce this result by showing that satisfiability of unrestricted QPTL^h is in fact h -EXPSPACE-hard.

number in $[0, \text{Tower}(1, n) - 1]$ (recall that $\text{Tower}(1, n) = 2^n$) whose binary code is $b_1 \dots b_n$ (we assume that b_1 is the least significant bit).

Induction Step: let $h \geq 1$. An $(h+1, n)$ -code is a word w over AP_{h+1} of the form

$$\$_{h+1} b \$_h w_1 \$_h w_2 \$_h \dots \$_h w_{\text{Tower}(h, n)} \$_h \$_{h+1}$$

where $b \in \{0, 1\}$ and for all $i \in [1, \text{Tower}(h, n)]$, $\$_h w_i \$_h$ is an (h, n) -code whose index is $i - 1$. Let b_i be the content of the (h, n) -code $\$_h w_i \$_h$. Then, the *content* of w is the bit b , and the *index* of w is the natural number in $[0, \text{Tower}((h+1) - 1)]$ whose binary code is given by $b_1 \dots b_{\text{Tower}(h, n)}$.

Given a finite alphabet Σ such that $\text{AP} \cap \Sigma = \emptyset$, we also introduce the notion of (h, n) -block over Σ which is defined as an (h, n) -code but we require that the content is a symbol in Σ . The index of an (h, n) -block over Σ is defined as the index of an (h, n) -code. Intuitively, (h, n) -blocks are used to encode the cells of the configurations reachable by $\exp[h]$ -space bounded deterministic Turing machines on inputs of size n .

► **Example 38.** Let $n = 2$ and $h = 2$. In this case $\text{Tower}(h, n) = 16$ and $\text{Tower}(h-1, n) = 4$. Thus, we can encode by $(2, 2)$ -codes all the integers in $[0, 15]$. For example, let us consider the number 14 whose binary code (using $\text{Tower}(h-1, n) = 4$ bits) is given by 0111 (assuming that the first bit is the least significant one). The $(2, 2)$ -code with content 0 encoding number 14 is given by

$$\$_2 0 \$_1 0 00 \$_1 1 10 \$_1 1 01 \$_1 1 11 \$_1 \$_2$$

Note that we encode also the position of each bit in the binary code of 14.

Let Tag be an extra infinite set of atomic propositions disjoint from AP given by

$$\text{Tag} := \{bl, first, last\} \cup \{beg_1, end_1, beg_2, end_2, \dots\}$$

and for each $h \geq 1$, let Tag_h be the finite subset of Tag given by

$$\text{Tag}_h := \{bl, first, last\} \cup \{beg_1, end_1, \dots, beg_h, end_h\}$$

Intuitively, we use the propositions in Tag_h to mark (h, n) -blocks.

For all $h \geq 1$, the lower bound for satisfiability of existential QPTL^h is crucially based on the following Propositions 39 and 40. For a set P and a word w over $2^{P'}$ with $P' \supseteq P$, we say that w is P -simple if for each position i of w , $w(i) \cap P$ is a singleton.

► **Proposition 39.** For all $n \geq 1$ and $h \geq 1$, one can construct in time polynomial in n and h three existential QPTL^h formulas $\psi_{bl}(h, n)$, $\psi_{=}(h, n)$, and $\psi_{inc}(h, n)$ over $\text{AP}_h \cup \text{Tag}_h$ using only temporal modalities in $\{X, X^-, F, F^-, G, G^-\}$ such that for all AP_h -simple pointed words (w, i) , the following holds:

- $(w, i) \models \psi_{bl}(h, n) \Leftrightarrow$ there is $j > i$ such that $w[i, j]$ encodes an (h, n) -code.
 - Let $j > i$ such that
 - the projection of $w[i, j]$ over AP_h is of the form $\$_h w_1 \$_h w' \$_h w_2 \$_h$, where $\$_h w_1 \$_h$ and $\$_h w_2 \$_h$ are (h, n) -codes, and
 - the beginning and the end of $\$_h w_1 \$_h$ and $\$_h w_2 \$_h$ are marked by beg_h and end_h , respectively, and no other position of w is marked by beg_h and end_h .
- Then, $(w, i) \models \psi_{=}(h, n) \Leftrightarrow \$_h w_1 \$_h$ and $\$_h w_2 \$_h$ have the same index.

- Let $j > i$ such that the projection of $w[i, j]$ over AP_h has the form $\$_h w_1 \$_h w_2 \$_h$ so that $\$_h w_1 \$_h$ and $\$_h w_2 \$_h$ are (h, n) -codes. Then, $(w, i) \models \psi_{inc}(h, n) \Leftrightarrow$ there is $i \in [0, \text{Tower}(h, n) - 2]$ such that the index of $\$_h w_1 \$_h$ is i and the index of $\$_h w_2 \$_h$ is $i + 1$. Moreover, each existential quantifier in $\psi_{=}(h, n)$ is in the scope of some temporal modality.

Proof. Fix $n \geq 1$. For each $h \geq 1$, the construction of formulas $\psi_{bl}(n, h)$, $\psi_{=}(n, h)$, and $\psi_{inc}(h, n)$ is given by induction on h . Since n is fixed, for clarity of presentation, we write ψ_{bl}^h , $\psi_{=}^h$, and ψ_{inc}^h instead of $\psi_{bl}(h, n)$, $\psi_{=}(h, n)$, and $\psi_{inc}(h, n)$, respectively.

Base Step: $h = 1$

$$\psi_{bl}^1 := \$_1 \wedge X^{n+2} \$_1 \wedge \bigwedge_{i=1}^{n+1} X^i (0 \vee 1)$$

$$\psi_{=}^1 := \bigwedge_{i=1}^n \bigvee_{b \in \{0,1\}} X^{i+1} (b \wedge F(\text{end}_1 \wedge F(\text{beg}_1 \wedge X^{i+1} b)))$$

$$\psi_{inc}^1 := X \bigvee_{i=1}^n \left(\left[\bigwedge_{j=1}^{i-1} X^j (1 \wedge X^{n+2} 0) \right] \wedge \left[X^i (0 \wedge X^{n+2} 1) \right] \wedge \left[\bigwedge_{j=i+1}^n \bigvee_{b \in \{0,1\}} X^j (b \wedge X^{n+2} b) \right] \right)$$

Induction Step: let $h \geq 1$. In order to construct the formulas ψ_{bl}^{h+1} , $\psi_{=}^{h+1}$, and ψ_{inc}^{h+1} , for a proposition p , we use the following PLTL formulas $\theta(1, p)$ and $\theta(2, p)$, which are satisfied by a pointed word (w, i) iff there are at most one position and two positions, respectively, along w where p holds.

$$\begin{aligned} \theta(1, p) &:= F^-((\neg X^- \top) \wedge G(p \rightarrow XG \neg p)) \\ \theta(2, p) &:= F^-((\neg X^- \top) \wedge G(p \rightarrow XG(p \rightarrow XG \neg p))) \end{aligned}$$

Definition of formula ψ_{bl}^{h+1} .

$$\psi_{bl}^{h+1} := \exists bl. \exists first. \exists last. \left(\psi_h^{h+1} \wedge \psi_{first}^{h+1} \wedge \psi_{last}^{h+1} \wedge \psi_{suc}^{h+1} \right)$$

where

- ψ_h^{h+1} is an existential QPTL ^{$h+1$} formula which uses ψ_{bl}^h and requires that for the given AP_{h+1} -simple pointed word (w, i) , there is $j \geq i$ such that the projection of $w[i, j]$ over AP_{h+1} is of the form $\$_{h+1} b \$_h w_1 \$_h \dots \$_h w_p \$_h \$_{h+1}$, where $b \in \{0, 1\}$ and for each $i \in [1, p]$, $\$_h w_i \$_h$ is an (h, n) -code; we use existential quantification over bl to mark exactly the first and the last position of $w[i, j]$ by proposition bl .
- ψ_{first}^{h+1} and ψ_{last}^{h+1} are PLTL formulas: the first one requires that the index of the first (h, n) -code $\$_h w_1 \$_h$ of $w[i, j]$ is 0, and the second one requires that the index of the last (h, n) -code $\$_h w_p \$_h$ of $w[i, j]$ is $\text{Tower}(h, n) - 1$; we use existential quantification over $first$ and $last$ to mark the first and the last position of $\$_h w_1 \$_h$ by $first$, and the first and last position of $\$_h w_p \$_h$ by $last$.
- ψ_{suc}^{h+1} is an existential QPTL ^{$h+1$} formula using ψ_{inc}^h and requiring that for consecutive (h, n) -codes along $w[i, j]$, the index is incremented.

$$\begin{aligned} \psi_h^{h+1} &:= \theta(2, bl) \wedge bl \wedge \$_{h+1} \wedge XF(bl \wedge \$_{h+1}) \wedge XG((XFbl) \rightarrow \neg \$_{h+1}) \wedge X(0 \vee 1) \wedge \\ &\quad X^2 \$_h \wedge X^3 \neg \$_{h+1} \wedge \underbrace{XG((\$_h \wedge X(\neg \$_{h+1} \wedge Fbl)) \rightarrow \psi_{bl}^h)}_{\text{check that the } bl\text{-marked prefix is a sequence of } (h, n)\text{-codes}} \end{aligned}$$

check that the bl -marked prefix is a sequence of (h, n) -codes

$$\begin{aligned}
 \psi_{first}^{h+1} &:= \begin{cases} X^3 \bigwedge_{i=1}^n X^i 0 & \text{if } h = 1 \\ \theta(2, first) \wedge X^2 first \wedge X^3 F(first \wedge \$h) \wedge \\ X^3 G((XF first) \rightarrow \neg \$h) \wedge X^3 G((\$_{h-1} \wedge X^2 F first) \rightarrow X 0) & \text{otherwise} \end{cases} \\
 \psi_{last}^{h+1} &:= \begin{cases} \theta(2, last) \wedge F(last \wedge \$h \wedge XF(last \wedge \$h \wedge Xbl)) \wedge \\ G((X^- F^- last) \wedge X^2 F last) \longrightarrow X 1 & \text{if } h = 1 \\ G((X^- F^- last) \wedge XF last) \longrightarrow (\neg \$h \wedge ((\$_{h-1} \wedge \neg X \$h) \rightarrow X 1)) & \text{otherwise} \end{cases} \\
 \psi_{suc}^{h+1} &:= \underbrace{G((\$h \wedge XF(last \wedge XF last)) \longrightarrow \psi_{inc}^h)}_{\text{check that for consecutive } (h, n)\text{-codes the index is incremented}}
 \end{aligned}$$

Definition of formula ψ_{\equiv}^{h+1} .

$$\begin{aligned}
 \psi_{\equiv}^{h+1} &:= XG \left[(\$h \wedge X^2 F(end_{h+1} \wedge F beg_{h+1})) \longrightarrow \exists beg_h. \exists end_h. (\theta(2, beg_h) \wedge \theta(2, end_h) \wedge \right. \\
 &\quad \underbrace{\{ beg_h \wedge XF(end_h \wedge \$h \wedge X^- G^-((X^- F^- beg_h) \rightarrow \neg \$h)) \}}_{\text{mark the current } (h, n)\text{-code of the first } (h+1, n)\text{-code}} \wedge \\
 &\quad \underbrace{\{ F(beg_{h+1} \wedge F(beg_h \wedge \$h \wedge XF(end_h \wedge \$h \wedge F end_{h+1})) \wedge XG((XF end_h) \rightarrow \neg \$h)) \}}_{\text{select an } (h, n)\text{-code of the second } (h+1, n)\text{-code}} \wedge \\
 &\quad \underbrace{\{ \psi_{\equiv}^h \wedge \bigvee_{b \in \{0,1\}} (Xb \wedge XF(beg_h \wedge Xb)) \}}_{\text{check that the two selected } (h, n)\text{-codes have the same content and index; note that we use } \psi_{\equiv}^h}
 \end{aligned}$$

Note that ψ_{\equiv}^{h+1} ensures by using the always modality that each (h, n) -code of the first $(h+1, n)$ -code is selected.

Definition of formula ψ_{inc}^{h+1} . Let (w, i) be an AP_{h+1} -simple pointed word and $j \geq i$ such that the projection of $w[i, j]$ over AP_{h+1} is of the form $\$_{h+1} w_1 \$_{h+1} w_2 \$_{h+1}$, where $\$_{h+1} w_1 \$_{h+1}$ and $\$_{h+1} w_2 \$_{h+1}$ are $(h+1, n)$ -codes. Then, the requirement that there is $\ell \in [0, \text{Tower}(h+1, n) - 2]$ such that the index of $\$_{h+1} w_1 \$_{h+1}$ is ℓ and the index of $\$_{h+1} w_2 \$_{h+1}$ is $\ell + 1$ is equivalent to the following requirement

- there is a (h, n) -code bl of $\$_{h+1} w_1 \$_{h+1}$ such that denoting with bl' the (h, n) -code of $\$_{h+1} w_2 \$_{h+1}$ having the same index as bl , it holds that: (1) the content of bl is 0 and the content of each (h, n) -code of $\$_{h+1} w_1 \$_{h+1}$ that precedes bl is 1, (2) the content of bl' is 1 and the content of each (h, n) -code of $\$_{h+1} w_2 \$_{h+1}$ that precedes bl' is 0, and (3) each (h, n) -code bl_s of $\$_{h+1} w_1 \$_{h+1}$ that follows bl has the same content as the (h, n) -code of $\$_{h+1} w_2 \$_{h+1}$ having the same index as bl_s .

Thus, formula ψ_{inc}^{h+1} uses ψ_{\equiv}^h and is defined as follows. Note that we use existential quantification over bl to mark the first position of the (guessed) first (h, n) -code of the first $(h+1, n)$ -code whose content is 0. Moreover, we use existential quantification over $first$ and $last$ to mark by $first$, the first and the last position of the first $(h+1, n)$ -code, and by $last$, the first and the last position of the second $(h+1, n)$ -code.

$$\psi_{inc}^{h+1} := \exists first. \exists last. \exists bl. (\psi_{mark}^{h+1} \wedge \psi_{check}^{h+1})$$

$$\begin{aligned}
\psi_{mark}^{h+1} &:= \theta(2, first) \wedge \theta(2, last) \wedge \theta(1, bl) \wedge \\
&\quad \underbrace{first \wedge XF(first \wedge \$_{h+1}) \wedge XG((XF first) \rightarrow \neg \$_{h+1})}_{\text{mark with } first \text{ the beginning and the end of the first } (h+1, n)\text{-code}} \wedge \\
&\quad \underbrace{XF(first \wedge last \wedge XF(last \wedge \$_{h+1})) \wedge XG((XF last) \rightarrow \neg \$_{h+1}))}_{\text{mark with } last \text{ the beginning and the end of the second } (h+1, n)\text{-code}} \wedge \\
&\quad \underbrace{XF(bl \wedge \$_h \wedge X^2 F first)}_{\text{mark with } bl \text{ the beginning of some } (h, n)\text{-code of the first } (h+1, n)\text{-code}} \\
\psi_{check}^{h+1} &:= G \left((\$ _h \wedge X^2 F first) \rightarrow \exists beg_h. \exists end_h. \left\{ \theta(2, beg_h) \wedge \theta(2, end_h) \wedge \right. \right. \\
&\quad \underbrace{beg_h \wedge XF(end_h \wedge \$ _h \wedge XF first \wedge X^- G^- ((X^- F^- beg_h) \rightarrow \neg \$ _h))}_{\text{mark with } beg_h \text{ and } end_h \text{ the current } (h, n)\text{-code } cod_1 \text{ of the first } (h+1, n)\text{-code}} \\
&\quad \wedge \\
&\quad \underbrace{XF(first \wedge XF(beg_h \wedge \$ _h \wedge XF last \wedge XF(end_h \wedge \$ _h)) \wedge XG((XF end_h) \rightarrow \neg \$ _h))}_{\text{mark with } beg_h \text{ and } end_h \text{ some } (h, n)\text{-code } cod_2 \text{ of the second } (h+1, n)\text{-code}} \\
&\quad \wedge \\
&\quad \underbrace{\psi_{=}^h}_{\text{check that } cod_1 \text{ and } cod_2 \text{ have the same index}} \\
&\quad \wedge \\
&\quad \underbrace{(bl \rightarrow (X0 \wedge XF(beg_h \wedge X1)))}_{\text{if } cod_1 \text{ is the } (h, n)\text{-code marked by } bl, \text{ the contents of } cod_1 \text{ and } cod_2 \text{ are 0 and 1}} \\
&\quad \wedge \\
&\quad \underbrace{(XF bl \rightarrow (X1 \wedge XF(beg_h \wedge X0)))}_{\text{if } cod_1 \text{ precedes the } (h, n)\text{-code marked by } bl, \text{ the contents of } cod_1 \text{ and } cod_2 \text{ are 1 and 0}} \\
&\quad \wedge \\
&\quad \underbrace{(X^- F^- bl \rightarrow \bigvee_{b \in \{0,1\}} (Xb \wedge XF(beg_h \wedge Xb)))}_{\text{if } cod_1 \text{ follows the } (h, n)\text{-code marked by } bl, \text{ the contents of } cod_1 \text{ and } cod_2 \text{ coincide}} \left. \right\}
\end{aligned}$$

By construction, it easily follows that the sizes of ψ_{bl}^h , $\psi_{=}^h$, ψ_{inc}^h are polynomial in n and h , ψ_{bl}^h , $\psi_{=}^h$, and ψ_{inc}^h are $QPTL^h$ formulas, and each existential quantifier in $\psi_{=}^h$ is in the scope of some temporal modality. This concludes the proof of Proposition 39. \blacktriangleleft

By a straightforward adaptation of the proof of Proposition 39, we obtain the following result.

► **Proposition 40.** *For all $n \geq 1$, $h \geq 1$, and finite alphabets Σ , one can construct in time polynomial in n , h , and Σ three existential $QPTL^h$ formulas $\psi_{bl}(h, n, \Sigma)$, $\psi_{=}(h, n, \Sigma)$, and $\psi_{inc}(h, n, \Sigma)$ over $AP_h \cup Tag_h \cup \Sigma$ using only temporal modalities in $\{X, X^-, F, F^-, G, G^-\}$ such that for all $(AP_h \cup \Sigma)$ -simple pointed words (w, i) , the following holds:*

- $(w, i) \models \psi_{bl}(h, n, \Sigma) \Leftrightarrow$ *there is $j > i$ such that $w[i, j]$ encodes an (h, n) -block over Σ .*
- *Let $j > i$ such that*
 - *the projection of $w[i, j]$ over $AP_h \cup \Sigma$ is of the form $\$ _h w_1 \$ _h w' \$ _h w_2 \$ _h$, where $\$ _h w_1 \$ _h$ and $\$ _h w_2 \$ _h$ are (h, n) -blocks over Σ , and*

- the beginning and the end of $\$hw_1\$$ and $\$hw_2\$$ are marked by beg_h and end_h , respectively, and no other position of w is marked by beg_h and end_h .
- Then, $(w, i) \models \psi_=(h, n, \Sigma) \Leftrightarrow \$hw_1\$$ and $\$hw_2\$$ have the same index.
- Let $j > i$ such that the projection of $w[i, j]$ over $AP_h \cup \Sigma$ has the form $\$hw_1\$hw_2\$$ so that $\$hw_1\$$ and $\$hw_2\$$ are (h, n) -blocks over Σ . Then, $(w, i) \models \psi_{inc}(h, n, \Sigma) \Leftrightarrow$ there is $i \in [0, \text{Tower}(h, n) - 2]$ such that the index of $\$hw_1\$$ is i and the index of $\$hw_2\$$ is $i + 1$.

Moreover, each existential quantifier in $\psi_=(h, n, \Sigma)$ is in the scope of some temporal modality.

Now, we can establish for each $h \geq 1$, the lower bound for the existential fragment of QPTL^h .

► **Theorem 41.** *For each $h \geq 1$, satisfiability for the existential fragment of QPTL^h is $(h-1)$ -EXPSpace-hard even for formulas whose temporal modalities are in $\{X, X^-, F, F^-, G, G^-\}$.*

Proof. It is well-known that satisfiability of PLTL is PSPACE-complete even if the unique allowed temporal modalities are in $\{X, X^-, F, F^-, G, G^-\}$ [3].¹⁰ Since QPTL^1 subsumes PLTL, the result for $h = 1$ follows.

Now, we prove the result for $h + 1$ with $h \geq 1$ by a polynomial time reduction from the non-halting problem of $\exp[h]$ -space bounded deterministic Turing Machines (TM, for short). Fix such a TM $\mathcal{M} = \langle A, Q, q_0, \delta \rangle$ over the input alphabet A , and let $c \geq 1$ be a constant such that for each $\alpha \in A^*$, the space needed by \mathcal{M} on input α is bounded by $\text{Tower}(h, |\alpha|^c)$. Fix an input $\alpha \in A^*$ and let $n = |\alpha|^c$. Note that any reachable configuration of \mathcal{M} over α can be seen as a word $\alpha_1 \cdot (q, a) \cdot \alpha_2$ in $A^* \cdot (Q \times A) \cdot A^*$ of length $\text{Tower}(h, n)$, where $\alpha_1 \cdot a \cdot \alpha_2$ denotes the tape content, q the current state, and the reading head is at position $|\alpha_1| + 1$. If $\alpha = a_1 \dots a_r$ (where $r = |\alpha|$), then the initial configuration is given by $(q_0, a_1)a_2 \dots a_r \underbrace{\#\#\dots\#}_{\text{Tower}(h, n) - r}$, where $\#$ is the blank symbol. Let $C = u_1 \dots u_{\text{Tower}(h, n)}$ be a TM

configuration. For $1 \leq i \leq \text{Tower}(h, n)$, the value u'_i of the i^{th} cell of the \mathcal{M} -successor of C is completely determined by the values u_{i-1} , u_i and u_{i+1} (taking u_{i+1} for $i = \text{Tower}(h, n)$ and u_{i-1} for $i = 1$ to be some special symbol, say \perp). Let $\text{next}(u_{i-1}, u_i, u_{i+1})$ be our expectation for u'_i (this function can be trivially obtained from the transition function δ of \mathcal{M}).

Let $\Sigma = A \cup (Q \times A)$. We build in time polynomial in \mathcal{M} and n an existential QPTL^{h+1} formula $\varphi_{\mathcal{M}, \alpha}$ over $\Sigma \cup AP_{h+1} \cup \text{Tag}_h$ which is satisfiable iff \mathcal{M} does not halt on the input α . Moreover, $\varphi_{\mathcal{M}, \alpha}$ uses only temporal modalities in $\{X, X^-, F, F^-, G, G^-\}$. Hence, the theorem follows.

A TM configuration $C = u_1 \dots u_{\text{Tower}(h, n)}$ is encoded by the word over $\Sigma \cup AP_{h+1}$ given by

$$\$_{h+1}\$hw_1\$ \dots \$hw_{\text{Tower}(h, n)}\$ \$_{h+1}$$

where for each $i \in [1, \text{Tower}(h, n)]$, $\$hw_i\$$ is an (h, n) -block whose content is u_i (the i^{th} symbol of C) and whose index is $i - 1$.

Then, the formula $\varphi_{\mathcal{M}, \alpha}$ uses the existential QPTL^h formulas $\psi_{bl}(h, n, \Sigma)$, $\psi_=(h, n, \Sigma)$, and $\psi_{inc}(h, n, \Sigma)$ of Proposition 40, and is given by

$$\varphi_{\mathcal{M}, \alpha} = G \left(\bigvee_{p \in \Sigma \cup AP_{h+1}} (p \wedge \bigwedge_{p' \in (\Sigma \cup AP_{h+1}) \setminus \{p\}} \neg p') \right) \wedge \varphi_{conf} \wedge \varphi_{init} \wedge \varphi_{fair}$$

¹⁰ See references for the Appendix.

where: (i) the first conjunct checks that the given word is $\Sigma \cup \text{AP}_{h+1}$ -simple, (ii) the second conjunct φ_{conf} checks that the projection of the given word over $\Sigma \cup \text{AP}_{h+1}$ is an infinite sequence of TM configuration codes, (iii) the third conjunct ensures that the first TM configuration is the initial one, and (iv) the last conjunct guarantees that the sequence of TM configuration codes is faithful to the evolution of \mathcal{M} . The construction of φ_{init} is straightforward. Thus, we focus on φ_{conf} and φ_{fair} , which are existential QPTL^{*h+1*} formulas. In the construction, we also use the PLTL formulas $\theta(1, p)$ and $\theta(2, p)$ (for an atomic proposition p) in the proof of Proposition 39, which are satisfied by a pointed word (w, i) iff there are at most one position and two positions, respectively, along w where p holds. The existential QPTL^{*h+1*} formula φ_{conf} uses the existential QPTL^{*h*} formulas $\psi_{bl}(h, n, \Sigma)$ and $\psi_{inc}(h, n, \Sigma)$, and is defined as follows. We assume that $h > 1$ (the case for $h = 1$ is simpler).

$$\begin{aligned}
\varphi_{\text{conf}} := & \ \$_{h+1} \wedge \text{GF}\$_{h+1} \wedge \text{G}(\$_{h+1} \rightarrow (\text{X}\$_{h+1} \wedge \text{X}^2\neg\$_{h+1})) \wedge \text{XG}(\$_{h+1} \rightarrow \text{X}^-\$_{h+1}) \wedge \\
& \underbrace{\text{G}((\$_{h+1} \wedge \neg\text{X}\$_{h+1}) \rightarrow \psi_{bl}(h, n, \Sigma))}_{\text{for every subword of the form } \$_{h+1}w\$_{h+1}, w \text{ is a sequence of } (h, n)\text{-blocks}} \\
& \wedge \\
& \text{G}\left((\$_{h+1} \wedge \neg\text{X}\$_{h+1}) \rightarrow \right. \\
& \left. \underbrace{(\psi_{inc}(h, n, \Sigma) \vee \exists \text{last}. [\theta(1, \text{last}) \wedge \text{XF}(\text{last} \wedge \$_{h+1} \wedge \text{X}\$_{h+1}) \wedge \text{XG}((\text{XF last}) \rightarrow \neg\$_{h+1})])}_{\text{for consecutive } (h, n)\text{-blocks the index is incremented}}\right) \\
& \wedge \\
& \text{G}\left((\$_{h+1} \wedge \text{X}^-\$_{h+1}) \rightarrow \exists \text{first}. [\theta(1, \text{first}) \wedge \right. \\
& \left. \underbrace{\text{XF}(\text{first} \wedge \$_{h+1}) \wedge \text{XG}((\text{XF first}) \rightarrow \neg\$_{h+1}) \wedge \text{G}((\$_{h-1} \wedge \text{X}^2\text{F first}) \rightarrow \text{X}0)]}_{\text{the first } (h, n)\text{-block of a TM configuration code has index 0}}\right) \\
& \wedge \\
& \text{G}\left((\$_{h+1} \wedge \text{X}\$_{h+1}) \rightarrow \exists \text{last}. [\theta(1, \text{last}) \wedge \right. \\
& \left. \underbrace{\text{X}^-\text{F}^-(\text{last} \wedge \$_{h+1}) \wedge \text{X}^-\text{G}^-(\text{X}^-\text{F}^-\text{last}) \rightarrow \neg\$_{h+1}) \wedge \text{X}^-\text{X}^-\text{G}^-(\$_{h-1} \wedge \text{F}^-\text{last}) \rightarrow \text{X}1)]}_{\text{the last } (h, n)\text{-block of a TM configuration code has index Tower}(h, n)-1}\right)
\end{aligned}$$

Finally, we define the formula φ_{fair} , which uses the existential QPTL^{*h*} formula $\psi_{=}(h, n, \Sigma)$ of Proposition 40. For a word w encoding a sequence of TM configurations, we have to require that for each subword $\$_{h+1}w_1\$_{h+1}w_2\$_{h+1}$, where $\$_{h+1}w_1\$_{h+1}$ and $\$_{h+1}w_2\$_{h+1}$ encode two TM configurations C_1 and C_2 , C_2 is the TM successor of C_1 , i.e., for each (h, n) -block bl' of $\$_{h+1}w_2\$_{h+1}$, the content u' of bl' satisfies $u' = \text{next}_{\mathcal{M}}(u_p, u, u_s)$, where u is the content of the (h, n) -block bl of $\$_{h+1}w_1\$_{h+1}$ having the same index as bl' , and u_p (resp., u_s) is the content of the (h, n) -block of $\$_{h+1}w_1\$_{h+1}$, if any, that precedes (resp., follows) bl . Note that $u_p = \perp$ (resp., $u_s = \perp$) iff bl is the first (resp., the last) (h, n) -block of $\$_{h+1}w_1\$_{h+1}$.¹¹

$$\varphi_{\text{fair}} := \bigwedge_{u \in \Sigma} \text{G}\left((\$_{h+1} \wedge \text{X}u) \rightarrow \bigvee_{u_p, u_s \in \Sigma \cup \{\perp\}} \phi_{u_p, u, u_s}\right)$$

where ϕ_{u_p, u, u_s} uses $\psi_{=}(h, n, \Sigma)$ and is defined as follows. Here, we only consider the case

¹¹ Since the first configuration is the initial one (this is ensured by φ_{init}), φ_{fair} also ensures that for each TM configuration code C , there is exactly one (h, n) -block of C whose content is in $Q \times A$.

where $u_p \neq \perp$ and $u_s \neq \perp$ (the other cases being similar).

$$\begin{aligned}
 \phi_{u_p, u, u_s} &:= \exists beg_h. \exists end_h. \exists first. \exists last \left\{ \theta(2, beg_h) \wedge \theta(2, end_h) \wedge \theta(1, first) \wedge \theta(1, last) \wedge \right. \\
 &\quad \underbrace{F(\$_{h+1} \wedge first) \wedge G((XF first) \rightarrow \neg \$_{h+1})}_{\text{mark with } first \text{ the end of the current TM configuration}} \\
 &\quad \wedge \\
 &\quad \underbrace{F(first \wedge XF(last \wedge \$_{h+1} \wedge X^- G^- ((X^- F^- first) \rightarrow \neg \$_{h+1})))}_{\text{mark with } last \text{ the end of the next TM configuration}} \\
 &\quad \wedge \\
 &\quad \underbrace{beg_h \wedge XF(end_h \wedge \$_h \wedge X^- G^- ((X^- F^- beg_h) \rightarrow \neg \$_h))}_{\text{mark with } beg_h \text{ and } end_h \text{ the current } (h, n)\text{-block } bl \text{ of the current TM configuration}} \\
 &\quad \wedge \\
 &\quad \underbrace{XF(first \wedge XF(beg_h \wedge \$_h \wedge XF last \wedge XF(end_h \wedge \$_h) \wedge XG((XF end_h) \rightarrow \neg \$_h)))}_{\text{mark with } beg_h \text{ and } end_h \text{ some } (h, n)\text{-block } bl' \text{ of the next TM configuration}} \\
 &\quad \wedge \\
 &\quad \underbrace{\psi_=(h, n, \Sigma) \wedge XF(beg_h \wedge X next(u_p, u, u_s))}_{\text{check that } bl \text{ and } bl' \text{ have the same index and the content of } bl' \text{ is } next(u_p, u, u_s)} \\
 &\quad \wedge \\
 &\quad \underbrace{X^- F^- (\$_h \wedge (X u_p) \wedge XG(XF(beg_h \wedge XF beg_h) \rightarrow \neg \$_h))}_{\text{check that the } (h, n)\text{-block preceding } bl \text{ has content } u_p} \\
 &\quad \wedge \\
 &\quad \left. \underbrace{F(end_h \wedge (X u_s) \wedge XF beg_h)}_{\text{check that the } (h, n)\text{-block following } bl \text{ has content } u_s} \right\}
 \end{aligned}$$

By Proposition 40, each existential quantifier in $\psi_=(h, n, \Sigma)$ is in the scope of some temporal modality. Hence, by construction, φ_{fair} is an existential QPTL^{*h*+1} formula. This concludes the proof of the theorem. \blacktriangleleft

B.5 Proof of Theorem 20

For a QPTL formula φ and $AP' \subseteq AP$ with $AP' = \{p_1, \dots, p_n\}$, we write $\exists AP'. \varphi$ to mean $\exists p_1. \dots \exists p_n. \varphi$. A QPTL sentence is a QPTL formula such that each proposition p occurs in the scope of a quantifier binding p .

► **Theorem 20.** *For all $h \geq 1$ and HyperCTL_{lp}^{*} sentences φ with strong alternation depth at most h , model-checking against φ is h -EXPSPACE-complete, and $(h-1)$ -EXPSPACE-complete in case φ is existential (even if the allowed temporal modalities are in $\{X, X^-, F, F^-, G, G^-\}$).*

Both the lower bounds and the upper bounds of Theorem 20 are based on Theorem 16. Without loss of generality, we only consider *well-named* QPTL (resp., HyperCTL_{lp}^{*} formulas), i.e., QPTL (resp., HyperCTL_{lp}^{*} formulas) where each quantifier introduces a different proposition (resp., path variable). Moreover, note that Theorem 16 holds even if we restrict ourselves to consider QPTL sentences.

Upper bounds of Theorem 20. We show that given a finite Kripke structure K and a well-named HyperCTL_{lp}^{*} sentence φ , one can construct in linear time a QPTL sentence φ' such that φ' is satisfiable iff K satisfies φ . Moreover, φ' has the same strong alternation

depth as φ , φ' is existential if φ is existential, and φ' uses only temporal modalities in $\{X, X^-, F, F^-, G, G^-\}$ if the same holds for φ . Hence, by Theorem 16, the upper bounds follow. Now, we give the details of the reduction.

Fix a finite Kripke structure $K = \langle S, s_0, E, V \rangle$ over AP. We consider a new finite set AP' of atomic propositions defined as follows:

$$AP' := \bigcup_{x \in \text{VAR}} AP_x \cup S_x \text{ where } AP_x := \{p_x \mid p \in AP\} \text{ and } S_x := \{s_x \mid s \in S\}$$

Thus, we associate to each variable $x \in \text{VAR}$ and atomic proposition $p \in AP$, a fresh atomic proposition p_x , and to each variable $x \in \text{VAR}$ and state s of K , a fresh atomic proposition s_x . For each $x \in \text{VAR}$ and initial path $\pi = s_0, s_1, \dots$ of K , we denote by $w(x, \pi)$ the infinite word over $2^{AP_x \cup S_x}$, encoding π , defined as follows: for all $i \geq 0$,

$$w(x, \pi)(i) := \{(s_i)_x\} \cup \{p_x \mid p \in V(s_i)\}$$

We encode path assignments Π of K (over VAR) by infinite words $w(\Pi)$ over $2^{AP'}$ as follows: for all $x \in \text{VAR}$, the projection of $w(\Pi)$ over $S_x \cup AP_x$ is $w(x, \Pi(x))$.

Next, for all $x \in \text{VAR}$, we construct in linear time a PLTL formula $\theta(x, K)$ over $2^{AP_x \cup S_x}$ encoding the initial paths of K as follows:

$$\begin{aligned} \theta(x, K) := & F^- \left\{ (\neg X^- \top) \wedge \right. \\ & \left. (s_0)_x \wedge G \bigwedge_{s \in S} \left(s_x \rightarrow \left[\bigwedge_{p \in V(s)} p_x \wedge \bigwedge_{p \in AP \setminus V(s)} \neg p_x \wedge \bigwedge_{t \in S \setminus \{s\}} \neg t_x \wedge \bigvee_{t \in E(s)} X t_x \right] \right) \right\} \end{aligned}$$

where $E(s)$ denotes the set of successors of s in K . By construction, the following holds.

Claim 1: for all $x \in \text{VAR}$ and infinite pointed words (w, i) over $2^{AP'}$, $(w, i) \models \theta(x, K)$ iff there is an initial path π of K such that the projection of w over $S_x \cup AP_x$ is $w(x, \pi)$.

Finally, we inductively define a mapping f associating to each pair (x, ψ) consisting of a variable $x \in \text{VAR}$ and a *well-named* HyperCTL* formula ψ over AP and VAR such that there is no quantifier binding x which occurs in ψ , a QPTL formula $f(x, \psi)$ over $2^{AP'}$ as follows:¹²

- $f(x, \top) = \top$;
- $f(x, p[y]) = p_y$ for all $p \in AP$ and $x, y \in \text{VAR}$;
- $f(x, \neg \psi) = \neg f(x, \psi)$;
- $f(x, \psi_1 \wedge \psi_2) = f(x, \psi_1) \wedge f(x, \psi_2)$;
- $f(x, X\psi) = Xf(x, \psi)$;
- $f(x, X^-\psi) = X^-f(x, \psi)$;
- $f(x, \psi_1 \cup \psi_2) = f(x, \psi_1) \cup f(x, \psi_2)$;
- $f(x, \psi_1 \cup^-\psi_2) = f(x, \psi_1) \cup^-f(x, \psi_2)$;
- $f(x, \exists^G y. \psi) = \exists(AP_y \cup S_y). (\theta(y, K) \wedge f(y, \psi))$;
- $f(x, \exists y. \psi) = \exists(AP_y \cup S_y). (\theta(y, K) \wedge f(y, \psi) \wedge G^- \bigwedge_{s \in S} (s_x \leftrightarrow s_y))$.

By construction, $f(x, \psi)$ has size linear in ψ and has the same strong alternation depth as ψ . Moreover, $f(x, \psi)$ is a QPTL sentence if ψ is a HyperCTL*_{lp} sentence, $f(x, \psi)$ is existential if ψ is existential, and $f(x, \psi)$ uses only temporal modalities in $\{X, X^-, F, F^-, G, G^-\}$ if the same holds for ψ . Hence, by Theorem 16, the upper bounds of Theorem 20 directly follow from the following claim.

¹²Intuitively, x represents the current quantified path variable.

Claim 2: let $x \in \text{VAR}$, Π be a path assignment of K and ψ be a well-named HyperCTL_{lp}^* formula ψ over AP and VAR such that there is no quantifier binding x which occurs in ψ . Then, for all $i \geq 0$:

$$\Pi, x, i \models_K \psi \Leftrightarrow w(\Pi), i \models f(x, \psi)$$

Proof of Claim 2: Let $x \in \text{VAR}$, Π , and ψ as in the statement of the claim. The proof is by induction on $|\psi|$. The cases for the boolean connectives and the temporal modalities \mathbf{X} , \mathbf{X}^- , \mathbf{U} , and \mathbf{U}^- easily follow from the induction hypothesis. For the other cases, we proceed as follows:

- $\psi = p[y]$ for some $p \in \text{AP}$ and $y \in \text{VAR}$: we have that $\Pi, x, i \models_K p[y] \Leftrightarrow p \in \Pi(y)(i) \Leftrightarrow p_y \in w(y, \Pi(y))(i) \Leftrightarrow p_y \in w(\Pi)(i) \Leftrightarrow w(\Pi), i \models f(x, p[y])$. Hence, the result follows.
- $\psi = \exists y. \psi'$: by hypothesis, $x \neq y$. For the implication, $\Pi, x, i \models_K \psi \Rightarrow w(\Pi), i \models f(x, \psi)$, assume that $\Pi, x, i \models_K \psi$. Hence, there exists an initial path π of K such that $\pi[0, i] = \Pi(x)[0, i]$ and $\Pi[y \leftarrow \pi], y, i \models \psi'$. Since ψ is well-named, there is no quantifier binding y which occurs in ψ' . Hence, by the induction hypothesis, $w(\Pi[y \leftarrow \pi]), i \models f(y, \psi')$. Moreover, since $x \neq y$, by construction, the projections of $w(\Pi[y \leftarrow \pi])$ over $\text{AP}_x \cup S_x$ and $\text{AP}_y \cup S_y$, respectively, are $w(x, \Pi(x))$ and $w(y, \pi)$. Thus, since $\pi[0, i] = \Pi(x)[0, i]$, by Claim 1 in the proof of Theorem 20, it follows that

$$w(\Pi[y \leftarrow \pi]), i \models \theta(y, K) \wedge f(y, \psi') \wedge \mathbf{G}^- \bigwedge_{s \in S} (s_x \leftrightarrow s_y)$$

Since the projections of $w(\Pi[y \leftarrow \pi])$ and $w(\Pi)$ over $\text{AP}' \setminus (S_y \cup \text{AP}_y)$ coincide, we obtain that

$$w(\Pi), i \models \exists (\text{AP}_y \cup S_y). \left(\theta(y, K) \wedge f(y, \psi') \wedge \mathbf{G}^- \bigwedge_{s \in S} (s_x \leftrightarrow s_y) \right) = f(x, \psi)$$

and the result follows.

The converse implication $w(\Pi), i \models f(x, \psi) \Rightarrow \Pi, x, i \models_K \psi$ is similar, and we omit the details here.

- $\psi = \exists^G y. \psi'$: this case is similar to the previous one.

This concludes the proof of Claim 2. ◀

Lower bounds of Theorem 20. We show that given a well-named QPTL sentence φ over AP , one can construct in linear time a finite Kripke structure K_{AP} (depending only on AP) and a HyperCTL_{lp}^* sentence φ' such that φ is satisfiable iff K_{AP} satisfies φ' . Moreover, φ' has the same strong alternation depth as φ , φ' is existential if φ is existential, and φ' uses only temporal modalities in $\{\mathbf{X}, \mathbf{X}^-, \mathbf{F}, \mathbf{F}^-, \mathbf{G}, \mathbf{G}^-\}$ if the same holds for φ . Hence, by Theorem 16, the result follows. Now, we proceed with the details of the reduction.

Let $\text{AP}' = \text{AP} \cup \{\text{tag}\}$, where tag is a fresh proposition, and fix an ordering $\{p_1, \dots, p_n\}$ of the propositions in AP . First, we encode an infinite word w over 2^{AP} by an infinite word $\text{en}(w)$ over $2^{\text{AP}'}$ defined as follows: $w = w_0 \cdot w_1 \cdot \dots$, where for each $i \geq 0$, w_i (the encoding of the i^{th} symbol of w) is the finite word over $2^{\text{AP}'}$ of length $n+1$ given by $\{\text{tag}\}P_1 \dots P_n$, where $P_k = \{p_k\}$ if $p_k \in w(i)$, and $P_k = \emptyset$ otherwise (for all $k \in [1, n]$). Then, the finite Kripke structure $K_{\text{AP}} = \langle S, s_0, E, V \rangle$ has size linear in $|\text{AP}|$ and it is constructed in such a way that the set of traces of the initial paths of K_{AP} coincides with the set of the encodings $\text{en}(w)$ of the infinite words w over 2^{AP} . Formally, K_{AP} is defined as follows:

- $S = \{p_h, \bar{p}_h \mid h \in \{1, \dots, n\}\} \cup \{\text{tag}\}$ and $s_0 = \text{tag}$;

- E consists of the edges (p_k, p_{k+1}) , (p_k, \bar{p}_{k+1}) , (\bar{p}_k, p_{k+1}) and $(\bar{p}_k, \bar{p}_{k+1})$ for all $k \in [1, n-1]$, and the edges (tag, p_1) , (tag, \bar{p}_1) , (p_n, tag) , and (\bar{p}_n, tag) .
- $V(tag) = \{tag\}$ and $V(p_k) = \{p_k\}$ and $V(\bar{p}_k) = \emptyset$ for all $k \in [1, n]$.

Finally, we inductively define a mapping g associating to each pair (h, ψ) consisting of an index $h \in [1, n]$ ¹³ and a well-named QPTL formula ψ over AP such that there is no quantifier in ψ binding proposition p_h , a HyperCTL_{tp}^{*} formula $g(h, \psi)$ over AP' and VAR = $\{x_1, \dots, x_n\}$:

- $g(h, \top) = \top$;
- $g(h, p_i) = X^i p_i[x_h]$ for all $p_i \in \text{AP}$;
- $g(h, \neg\psi) = \neg g(h, \psi)$;
- $g(h, \psi_1 \wedge \psi_2) = g(h, \psi_1) \wedge g(h, \psi_2)$;
- $g(h, X\psi) = X^{n+1} g(h, \psi)$;
- $g(h, X^-\psi) = X^{-n-1} g(h, \psi)$;
- $g(h, \psi_1 \cup \psi_2) = (tag[x_h] \rightarrow g(h, \psi_1)) \cup (g(h, \psi_2) \wedge tag[x_h])$;
- $g(h, \psi_1 \cup^-\psi_2) = (tag[x_h] \rightarrow g(h, \psi_1)) \cup^-(g(h, \psi_2) \wedge tag[x_h])$;
- $g(h, \exists p_k.\psi) = \exists^G x_k. \left(g(k, \psi) \wedge F^-((\neg X^-\top) \wedge G \bigwedge_{j \in [1, n] \setminus \{k\}} (p_j[x_h] \leftrightarrow p_j[x_k])) \right)$.

By construction, $g(h, \psi)$ has size linear in ψ and has the same strong alternation depth as ψ . Moreover, $g(h, \psi)$ is a HyperCTL_{tp}^{*} sentence if ψ is a QPTL sentence, $g(h, \psi)$ is existential if ψ is existential, and $g(h, \psi)$ uses only temporal modalities in $\{X, X^-, F, F^-, G, G^-\}$ if the same holds for ψ . Hence, by Theorem 16, the lower bounds of Theorem 20 directly follow from the following claim, where for each $i \geq 0$, $s(i) := i \cdot (n+1)$. Intuitively, $s(i)$ is the tag -position associated with the $2^{\text{AP}'}$ -encoding of the position i of an infinite word over 2^{AP} .

Claim 3: Let ψ be a well-named QPTL formula ψ over AP and $h \in [1, n]$ such that there is no quantifier in ψ binding proposition p_h . Then, for all pointed words (w, i) over 2^{AP} and assignment maps Π of K_{AP} such that $V(\Pi(x_h)) = en(w)$,

$$(w, i) \models \psi \Leftrightarrow \Pi, x_h, s(i) \models_{K_{\text{AP}}} g(h, \psi)$$

Proof of Claim 3: let ψ , h , (w, i) , and Π as in the statement of the claim. The proof is by induction on $|\psi|$. The cases for the boolean connectives easily follow from the induction hypothesis. For the other cases, we proceed as follows:

- $\psi = p_j$ for some $p_j \in \text{AP}$: we have that $(w, i) \models p_j \Leftrightarrow p_j \in w(i) \Leftrightarrow p_j \in en(w)(s(i) + j) \Leftrightarrow p_j \in V(\Pi(x_h))(s(i) + j) \Leftrightarrow \Pi, x_h, s(i) \models_{K_{\text{AP}}} X^j p_j[x_h] \Leftrightarrow \Pi, x_h, s(i) \models_{K_{\text{AP}}} g(h, p_j)$. Hence, the result follows.
- $\psi = X\psi'$: we have that $(w, i) \models X\psi' \Leftrightarrow (w, i+1) \models \psi' \Leftrightarrow$ (by the induction hypothesis) $\Pi, x_h, s(i+1) \models_{K_{\text{AP}}} g(h, \psi') \Leftrightarrow$ (since $s(i+1) = s(i) + n + 1$) $\Pi, x_h, s(i) \models_{K_{\text{AP}}} X^{n+1} g(h, \psi') \Leftrightarrow \Pi, x_h, s(i) \models_{K_{\text{AP}}} g(h, X\psi')$. Hence, the result follows.
- $\psi = X^-\psi'$: similar to the previous case.
- $\psi = \psi_1 \cup \psi_2$: we have that $(w, i) \models \psi_1 \cup \psi_2 \Leftrightarrow$ there is $t \geq i$ such that $(w, t) \models \psi_2$ and $(w, r) \models \psi_1$ for all $i \leq r < t \Leftrightarrow$ (by the induction hypothesis) there is $t \geq i$ such that $\Pi, x_h, s(t) \models_{K_{\text{AP}}} g(h, \psi_2)$ and $\Pi, x_h, s(r) \models_{K_{\text{AP}}} g(h, \psi_1)$ for all $i \leq r < t \Leftrightarrow$ there is $t' \geq s(i)$ such that $\Pi, x_h, t' \models_{K_{\text{AP}}} g(h, \psi_2)$ and $tag \in V(\Pi(x_h))(t')$, and for all $s(i) \leq r' < t'$ such that $tag \in V(\Pi(x_h))(r')$, $\Pi, x_h, r' \models_{K_{\text{AP}}} g(h, \psi_1) \Leftrightarrow \Pi, x_h, s(i) \models_{K_{\text{AP}}} g(h, \psi_1 \cup \psi_2)$. Hence, the result follows.

¹³ intuitively, p_h represents the current quantified proposition.

- $\psi = \psi_1 \mathbf{U}^- \psi_2$: similar to the previous case.
- $\psi = \exists p_k. \psi'$: by hypothesis, $k \neq h$. For the implication, $(w, i) \models \psi \Rightarrow \Pi, x_h, s(i) \models_{K_{AP}} g(h, \psi)$, assume that $(w, i) \models \psi$. Hence, there exists a pointed word (w', i) such that $w' =_{AP \setminus \{p_k\}} w$ and $(w', i) \models \psi'$. Let π' be the initial path of K_{AP} such that $V(\pi') = en(w')$. Since ψ is well-named, there is no quantifier of ψ' binding proposition p_k . Thus, by the induction hypothesis,

$$\Pi[x_k \leftarrow \pi'], x_k, s(i) \models_{K_{AP}} g(k, \psi')$$

Moreover, since $V(\Pi[x_h]) = en(w)$, it holds that for all positions $\ell \geq 0$ and propositions $p_j \in AP \setminus \{p_k\}$, $p_j \in V(\Pi(x_h)(\ell))$ iff $p_j \in V(\Pi[x_k \leftarrow \pi'](x_k)(\ell))$. Thus, since $h \neq k$, it holds that

$$\Pi[x_k \leftarrow \pi'], x_k, s(i) \models_{K_{AP}} F^-((\neg X^- \top) \wedge G \bigwedge_{j \in [1, n] \setminus \{k\}} (p_j[x_h] \leftrightarrow p_j[x_k]))$$

By construction, it follows that $\Pi, x_h, s(i) \models_{K_{AP}} g(h, \exists p_k. \psi')$, and the result follows. The converse implication $\Pi, x_h, s(i) \models_{K_{AP}} g(h, \psi) \Rightarrow (w, i) \models \psi$ is similar, and we omit the details here.

This concludes the proof of Claim 3. ◀

References

- 1 O. Kupferman and M.Y. Vardi. Weak alternating automata are not that weak. *ACM Transactions on Computational Logic*, 2(3):408–429, 2001.
- 2 S. Miyano and T. Hayashi. Alternating finite automata on ω -words. *Theoretical Computer Science*, 32:321–330, 1984.
- 3 M.Y. Vardi. A temporal fixpoint calculus. In *Proc. 15th POPL*, pages 250–259. ACM, 1988.
- 4 W. Zielonka. Infinite games on finitely coloured graphs with applications to automata on infinite trees. *Theoretical Computer Science*, 200(1-2):135–183, 1998.